ACTA UNIVERSITATIS SZEGEDIENSIS

ACTA SCIENTIARUM MATHEMATICARUM

ADIUVANTIBUS

L. KALMÁR, L. RÉDEI ET K. TANDORI

REDIGIT

B. SZ.-NAGY

TOMUS XXI

FASC. 3—4

SZEGED, 1960

INSTITUTUM BOLYAIANUM UNIVERSITATIS SZEGEDIENSIS

A SZEGEDI TUDOMÁNYEGYETEM KÖZLEMÉNYEI

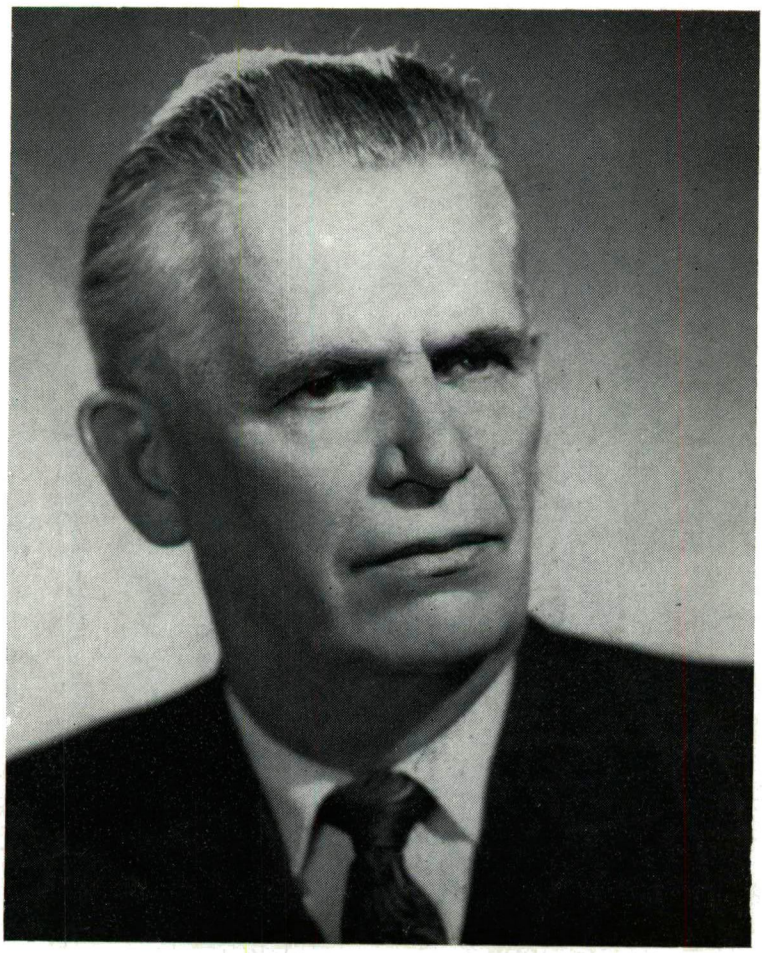
ACTA SCIENTIARUM MATHEMATICARUM

KALMÁR LÁSZLÓ, RÉDEI LÁSZLÓ ÉS TANDORI KÁROLY
KÖZREMŰKÖDÉSÉVEL
SZERKESZTI
SZŐKEFALVI-NAGY BÉLA

21. KÖTET
3—4. FÜZET

SZEGED, 1960. NOVEMBER HÓ

SZEGEDI TUDOMÁNYEGYETEM BOLYAI-INTÉZETE



RÉDEI LÁSZLÓ

Über die Gleichheit der Polynomfunktionen auf Ringen

Von J. ACZÉL in Debrecen

Herrn Professor Ladislaus Rédei zum 60. Geburtstag gewidmet

Bei der Bestimmung jener Polynome zweier Veränderlichen, die als Operationen betrachtet assoziativ sind (siehe z. B. [1]), macht man einzig von der Tatsache Gebrauch, daß zwei Polynome (dann und) nur dann gleich sind, wenn alle Koeffizienten übereinstimmen, oder — was auf dasselbe hinausgeht — aus

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \tag{1}$$

notwendigerweise

$$a_0 = a_1 = \cdots = a_{n-1} = a_n = 0 \tag{2}$$

folgt. Dies nennen wir das *Koeffizientenvergleichungsprinzip*. Hier werden die Polynome *als Funktionen* aufgefaßt, diese Betrachtungen gehören also zu dem von L. RÉDEI und T. SZELE [2] angegriffenen Problemkreis, wo solche Funktionen mit Anführungszeichen „Polynome" genannt werden. In [1] werden reelle (komplexe) Polynome betrachtet. Ich warf die Frage auf, in welchen Ringen diese Betrachtungen gültig bleiben, in welchen Ringen also das oben erwähnte Prinzip seine Gültigkeit behält (es seien außer der Veränderlichen etwa auch die Koeffizienten Ringelemente). Es war eine Überraschung für mich, als ich (u. a. von Prof. L. RÉDEI) hörte, daß diese als natürlich erscheinende Frage anscheinend noch nicht untersucht wurde.

So wage ich hier einen einfachen Satz zu beweisen, der eine hinreichende Bedingung für einen Ring angibt, damit in diesem Ring das Koeffizientenvergleichungsprinzip gelte. Die Frage bezüglich einer notwendigen und hinreichenden Bedingung werfe ich auch auf.

Die üblichen Schritte (Einsetzen von $x = 0$ um $a_n = 0$ zu konstatieren, dann Dividieren durch x oder Derivieren, wieder $x = 0$ zu setzen usw.), mit denen man im Reellen oder Komplexen aus (1) auf (2) folgert, sind in allgemeinen Ringen nicht oder nur unter sehr einschränkenden Bedingungen

durchführbar.[1]) Wir werden einen anderen Kunstgriff, den der Differenzenbildung anwenden und beweisen hiermit den folgenden

Satz. *Das Koeffizientenvergleichungsprinzip ist in jedem Ring mit Einselement gültig, dessen additive Gruppe torsionsfrei ist.*

Beweis. Offenbar genügt es zu beweisen, daß in solchen Ringen aus (1) das Bestehen von $a_0=0$ (bei jedem n) folgt, denn danach folgt auch aus $a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$ das Bestehen von $a_1=0$ usw. Weiter genügt es aus (1) eine Formel der Gestalt

$$na_0x^{n-1}+P_{n-2}=0 \tag{3}$$

zu folgern, wo P_{n-2} ein Polynom höchstens $(n-2)$-ten Grades ist, da hieraus durch wiederholte Anwendung $n!\,a_0=0$, also wegen der Torsionsfreiheit $a_0=0$ folgt.

Um (3) zu beweisen, setzen wir in (1) $x+e$ statt x ein, wo e das Einselement ist, dessen Existenz vorausgesetzt wurde. Da e mit jedem Ringelement vertauschbar ist, erhalten wir

$$a_0(x+e)^n+a_1(x+e)^{n-1}+\cdots+a_n=a_0x^n+na_0x^{n-1}+Q_{n-2}+a_1x^{n-1}+R_{n-2}=0,$$

wo Q_{n-2} und R_{n-2} Polynome höchstens $(n-2)$-ten Grades sind. Wenn wir hieraus (1) subtrahieren, erhalten wir einen Ausdruck der Gestalt (3), womit der Beweis beendet ist.

Bemerkungen. Falls (2) aus (1) nicht für alle n, sondern nur für alle $n\leqq N$, folgen soll, so genügt es vorauszusetzen, daß $N!$ kein Mehrfaches der (additiven) Ordnung des gegebenen Ringes mit Einselement ist (d. h. $N!\,a=0$ für kein Ringelement $a\neq 0$ bestehe). Dann können nämlich auch $(N-1)!$, $(N-2)!,\ldots,2!$ keine Mehrfache der Ordnung sein. — Unter den Voraus-

[1]) Ein weiteres Verfahren wäre das Einsetzen von $n+1$ verschiedenen Werten für x, womit man ein homogenes lineares Gleichungssystem für $a_0, a_1, \ldots, a_n$ erhielte, dessen Koeffizientenschema eine Vandermondeschen Matrix ist. Nun besteht aber vor der Bildung der Vandermondeschen Determinante, die dann nicht-verschwindend sein müßte, ein Hindernis, falls der Ring nicht kommutativ ist. — Nach Abschluß dieser Note hat L. Fuchs meine Aufmerksamkeit gefälligst darauf aufgerufen, daß dieser Gedankengang doch durchfürbar ist, falls wir r_ix $(i=0, 1, \ldots, n)$ für x einsetzen, wo die r_i ganze rationale Zahlen sind, deren Potenzen also mit allen Ringelementen vertauschbar sind, insbesondere mit den Koeffizienten und mit der Veränderlichen und natürlich auch miteinander. Also erhalten wir ein homogenes lineares Gleichungssystem für $a_0x^n, a_1x^{n-1}, \ldots, a_{n-1}x, a_n$ aus dessen Koeffizientenschema jetzt die Vandermondesche Determinante ohne Schwierigkeit gebildet werden kann, die, falls die r_i alle verschieden sind, nichtverschwindend ist. Deshalb ist $a_kx^{n-k}=0$, $(k=1, \ldots, n)$. Wenn es wenigstens einen Nicht-Nullteiler im Ringe gibt, so folgt $a_k=0$, $(k=0, 1, \ldots, n)$.

setzungen unseres Satzes scheint die der Existenz eines Einselementes nicht wesentlich, dagegen die der Torsionsfreiheit wesentlich zu sein.[2])

Ich bin den Herren Prof. BÉLA SZ.-NAGY und M. HOSSZÚ für wertvolle Anregungen zum Dank verpflichtet.

Schriftenverzeichnis

[1] E. T. BELL, A functional equation in arithmetic, *Transactions Amer. Math. Soc.*, **39** (1936), 341—344.

[2] L. RÉDEI—T. SZELE, Algebraisch-zahlentheoretische Betrachtungen über Ringe. I, *Acta Math.*, **79** (1947), 291—320.

(Eingegangen am 22. Juli 1959)

[2]) Bezüglich der Entbehrlichkeit des Einselementes s. [1]) und die nachstehende Note von M. Hosszú. — Bezüglich der Wesentlichkeit der Torsionsfreiheit kann erwähnt werden, daß es zu jeder (additiven) Ordnung Ringe dieser Ordnung gibt, in denen das Koeffizientenvergleichungsprinzip nicht gültig ist. Herr Z. PAPP hat bemerkt, daß sogar jeder endliche kommutative Ring (mit Einselement) ein solches Beispiel liefert: sind nämlich $0, c_1, c_2, \ldots, c_{n-1}$ die Elemente des Ringes, so ist $x(x+c_1)\ldots(x+c_{n-1}) = x^n + \cdots + c_1 c_2 \ldots c_{n-1} x$ ein Polynom das für jedes Ring element identisch verschwindet, ohne daß alle Koeffizienten gleich 0 wären. (Es gibt nämlich für jedes $x = c_k$ ein c_i derart, daß $c_k + c_i = 0$ gilt. Deshalb verschwindet unser Polynom, welches offenbar auch bei $x = 0$ gleich 0 ist, für jedes $x = c_k$, $k = 1, 2, \ldots, n-1$.)

Notes on vanishing polynomials

By MIKLÓS HOSSZÚ in Miskolc

To Professor László Rédei on his 60th birthday

It is known that there exist rings R in which a polynomial function

$$f_n(x) = a_n x^n + \cdots + a_1 x + a_0$$

can vanish identically even if not all coefficients a_k are equal to 0.[1])

Example 1. Let R_n be the ring of a complete residue system of integer numbers modulo n. Then we have

$$\prod_{k=1}^{n}(x-k) = a_n x^n + \cdots + a_0 \equiv 0 \pmod{n}$$

for all $x \in R_n$, however, $a_n = 1 \neq 0$. Observe that $nx \equiv 0 \pmod{n}$ is true for all $x \in R_n$.

Example 2. Let R_6 be the ring of a complete residue system of integer numbers modulo 6. Then we have

$$x(x-1)(x-2)(x-3)(x-5) \equiv x^5 + x^4 - x^3 - x^2 \equiv 0 \pmod{6}$$

for all $x \in R_6$. This is evident for $x = 0, 1, 2, 3, 5$ and also for $x = 4$ since we have

$$(4-2)(4-1) = 6 \equiv 0 \pmod{6}.$$

Observe that R_6 contains non zero elements of order 2 resp. 3 for which $2a \equiv 0$ resp $3a \equiv 0 \pmod{6}$ holds such that $a \not\equiv 0 \pmod{6}$.

There arises the problem[2]) to give conditions necessary and sufficient in order that in a ring R an identity

$$a_n x^n + \cdots + a_1 x + a_0 = b_n x^n + \cdots + b_1 x + b_0$$

---

[1]) Here $x \in R$, further, a_k is taken either from R or if $k \geqq 1$ from the integer numbers; e. g. $x^3 - x^2 + 2x + a_0$ is a polynomial. In the notation we shall take no distinction between the integer 0 and the zero element of R; this leads no to misunderstanding.

[2]) Cf. J. Aczél, Über die Gleichheit der Polynomfunktionen auf Ringen, *Acta Sci. Math.*, **21** (1960), 105—107. See also: Collected Math. Problems of the Inst. of Math. of Kossuth L. Univ. in Debrecen.

implies that the respective coefficients of the polynomials are equal: $a_k = b_k$ $(k = 0, 1, \ldots, n)$. It is clear that this is equivalent with the uniqueness of the identically vanishing polynomial on R. The main result of the present paper is:

Theorem. *Let R be a ring in which* (1) *R^+ does not contain any element of order $r \leqq n$ (up to 0). Then R has a unique identically vanishing polynomial of degree n if and only if* (2) *the set of elements of the form x^k $(x \in R)$ possesses a unique left anullator for every fixed $k = 1, \ldots, n$.*

Proof. The necessity of (2) is evident. On the other hand, in order to prove the sufficiency, let us suppose (2) on a ring R satisfying (1) and introduce the difference operator Δ_z^k by

$$\Delta_z^k = \Delta_z^{k-1}\Delta_z, \quad \Delta_z^1 f(x) = f(x+z) - f(x); \qquad x, y \in R.$$

Then

$$f_n(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0$$

implies

$$\Delta_z^n f_n(x) = n!\, a_n z^n \equiv 0.$$

Thus, by (2), we have $n!\, a_n z^n = 0$. But (1) involves the cancellability by $n, n-1, \ldots, 2$ and so we have $a_n = 0$. Now, applying the operator Δ_z^{n-1} for the identically vanishing polynomial $f_n(x) - a_n x^n$, in a similar way we get $a_{n-1} = 0$ and, successively, $a_{n-2} = \cdots = a_1 = 0$. Finally, by putting $x = 0$ into $f_n(x)$, we obtain also $a_0 = 0$.

The present proof makes use of the obvious fact that $\Delta_z^k x^k = k!\, z^k$ is true in an arbitrary ring R.

Remarks. **1.** Examples 1 and 2 show that without supposing (1) our theorem does not hold in general.

2. Since the order of an element is a divisor of the order of R, we have proved the

Corollary. *Let d denote the smallest prime divisor of n. Then R_n (see example 1) has exactly one identically vanishing polynomial of degree less than d.*

3. The condition (1) in our theorem can be replaced by the following one:

(1′) *For every $a \neq 0$ element in R and for arbitrary $i < k = 2, \ldots, n$ there exists at least one integer q such that for $p = q^k - q^i$ we have $pa \neq 0$.*

Then the sufficiency of (2) can be proved by successive application of the operator

$$\sigma_q^k f(x) = f(qx) - q^k f(x)$$

for

$$f_n(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0.$$

In fact, then we have

$$g_0(x) = f_n(x) - f_n(0) = a_n x^n + \cdots + a_1 x \equiv 0,$$
$$g_1(x) = \sigma_{q_1}^1 g_0(x) = (q_1^n - q_1) a_n x^n + \cdots + (q_1^2 - q_1) a_2 x^2 \equiv 0,$$
$$\cdots$$
$$g_{n-1}(x) = \sigma_{q_{n-1}}^{n-1} g_{n-2}(x) = (q_1^n - q_1)(q_2^n - q_2^2) \ldots a_n x^n \equiv 0$$

for all $x \in R$ and for every integer q_i. But this implies that $a_n x^n \equiv 0$ and, consequently, $a_n = 0$, further similarly, $a_{n-1} = \cdots = a_1 = 0$ are true.

Here (1'), i. e., the cancellability of $pa = 0$ by $p = q^k - q^i = q^i(q^{k-i} - 1)$ was used at least for one $p = p(a)$. Observe that this condition (1') is fulfilled e. g. if the cancellability by 2 and by $2^k - 1$ $(k = 2, \ldots, n-1)$ is supposed on R.

4. Problem. Give necessary and sufficient conditions under which a ring R possesses a unique identically (for all $x \in R$) vanishing polynomial of the form

$$f_n(x) = \sum_{k=1}^{n} (a_k x^k + x^k b_k)$$

resp.

$$g_n(x) = \sum_{k=1}^{n} \prod_{i=0}^{2k} z_{ik}(x)$$

of degree n, where a_k, b_k are fixed elements in R [3]) and

$$z_{ik}(x) = \begin{cases} a_{ik} \in R \text{ (constant), if } i \text{ is even,} \\ x \in R, \text{ otherwise.} \end{cases}$$

(Received August 27, 1959)

[3]) Or, more generally, it may be allowed that some of a_k, b_k, a_{ik} are integer numbers.

On the representation of integers as the sums of distinct summands taken from a fixed set

J. W. S. CASSELS in Cambridge (England)

To Professor L. Rédei on his 60th birthday

1. Introduction

Let $\mathfrak{A}$ be a sequence of distinct positive integers

$$a_1 < a_2 < a_3 < \cdots .$$

We write $A(n)$ for the number of elements a of $\mathfrak{A}$ with $a \leqq n$, and similarly for other sets. As usual, we put

$$\|x\| = \inf |x-n| \qquad (n = 0, \pm 1, \pm 2, \ldots).$$

We shall establish the following theorem:

Theorem I. *Suppose that*

$$\lim_{n\to\infty} \frac{A(2n)-A(n)}{\log\log n} = \infty \tag{*}$$

and that

$$\sum_{a\in\mathfrak{A}} \|a\theta\|^2 = \infty \tag{**}$$

for every real number θ in $0 < \theta < 1$. Then every sufficiently large number is representable as the sum of distinct elements of $\mathfrak{A}$.

We prove Theorem I in § 2 by the Hardy—Littlewood circle method. It will be seen that we do not use quite the full force of the hypotheses. By a more refined estimate of the integrals which occur, it would probably be possible to weaken the hypotheses further.

This investigation was touched off by the ingenious paper of BIRCH [1] about the representation of integers as the sums of the elements $p^\alpha q^\beta$ ($\alpha = 0, 1, 2, \ldots$; $\beta = 0, 1, 2, \ldots$), where p, q is a pair of coprime integers. His results are an immediate consequence of Theorem I.

In § 3 we shall prove the following result, which shows that congruence considerations and a very severe condition on the rate of increase of $A(n)$ are not alone sufficient to ensure that every sufficiently large number is the sum of distinct elements of $\mathfrak{A}$.

Theorem II. *Let $\varepsilon > 0$ be given. Then there exists a set $\mathfrak{C}$ of positive integers $c_1 < c_2 < \cdots$ with the following properties:*

(i) $$\lim_{n\to\infty} (c_{n+1} - c_n)/c_n^{\frac{1}{2}+\varepsilon} = 0;$$

(ii) *$\mathfrak{C}$ contains infinitely many elements in every arithmetic progression;*

(iii) *if $S(n)$ denotes the number of integers $\leqq n$ which are expressible as the sum of distinct elements of $\mathfrak{C}$, then $S(n) < \varepsilon n$ for every n.*

Note that (i) implies, in particular, that

$$\lim_{n\to\infty} n^{-\frac{1}{2}+\varepsilon} C(n) = \infty.$$

On the other hand, it is easy to see that any set $\mathfrak{A}$ with

$$\liminf n^{-2/3} A(n) > 0$$

satisfies condition $(\overset{*}{*})$ of Theorem I provided that $\mathfrak{A}$ contains infinitely many elements not divisible by any given integer $m > 1$.

[*Added in proof.* Since this was written, my attention has been drawn to the paper of ROTH and SZEKERES [7]. Their point of view is rather different from mine, since they are primarily interested in the behaviour of the number of representations. From their work it follows, in particular, that condition (*) may be weakened provided that condition $(\overset{*}{*})$ is appropriately strengthened. They do not require such delicate estimates of integrals as are needed in this paper.]

2. Proof of Theorem I

We shall not apply the Hardy—Littlewood method to the set $\mathfrak{A}$ directly, but to a subset $\mathfrak{B}$ of $\mathfrak{A}$. It will clearly be enough to show that every sufficiently large integer is the sum of distinct elements of $\mathfrak{B}$. The set $\mathfrak{B}$ is constructed in Lemma 1. It should perhaps be remarked that, while we have for convenience given explicit numerical values to constants occurring in the argument, we have made no attempt to make those values small and have estimated quite crudely.

Lemma 1. *There is a set* $\mathfrak{B} \subset \mathfrak{A}$ *and integers* M, N *with* $2^{40} \leqq N \leqq M$ *such that*

(i) $$\sum_{b \in \mathfrak{B},\, b \leqq 2^M} \|b\theta\|^2 > 2N + 50$$

for all real θ *in the range* $2^{-N-2} \leqq \theta \leqq 1 - 2^{-N-2}$,

(ii) $$B(2^{m+1}) - B(2^m) \geqq 2^{20} \log_2 m \quad (\textit{for all} \quad m \geqq N),$$

(iii) $$B(2^{m+1}) - B(2^m) \leqq 2^{20} \log_2 m + 1 \quad (\textit{for all} \quad m \geqq M),$$

where $\log_2 m = \log m / \log 2$.

First, by (i) of the enunciation of Theorem I there is an integer $N \geqq 2^{40}$ such that

(1) $$A(2n) - A(n) > 2^{20} \log_2 \log_2 n \quad (\text{for all} \quad n \geqq 2^N).$$

Secondly, by condition (ii) of Theorem I and a routine application of the Heine—Borel covering theorem, there is an integer $M \geqq N$ such that

$$\sum_{a \in \mathfrak{A},\, a \leqq 2^M} \|a\theta\|^2 > 2N + 50$$

for all θ in the range $2^{-N-2} \leqq \theta \leqq 1 - 2^{-N-2}$.

The elements b of the set $\mathfrak{B}$ in the range

$$0 < b \leqq 2^M$$

are taken to be just the elements of $\mathfrak{A}$ in that interval. The elements of $\mathfrak{B}$ in an interval

(2) $$2^m < b \leqq 2^{m+1} \qquad (m \geqq M)$$

are taken to be just any selection of

$$[2^{20} \log_2 m] + 1$$

of the elements of $\mathfrak{A}$ in that interval. (That there are so many elements of $\mathfrak{A}$ in (2) follows from (1).) The set $\mathfrak{B}$ so constructed clearly has all the required properties.

Let ϱ be a number in the range

$$0 < \varrho < 1$$

to be chosen later. The number of representations of an integer n by distinct summands from $\mathfrak{B}$ is clearly

$$\{2\pi\varrho^n\}^{-1} \int_{-\pi}^{\pi} \prod_{b \in \mathfrak{B}} (1 + \varrho^b e^{ib\vartheta}) e^{-in\theta} d\theta.$$

Hence to prove the theorem it will be enough to show that

$$\int_{-\pi}^{\pi} F(\theta) e^{-in\theta} d\theta \neq 0 \tag{3}$$

for all sufficiently large n, where

$$F(\theta) = \prod_{b \in \mathfrak{B}} \left(\frac{1 + \varrho^b e^{ib\theta}}{1 + \varrho^b} \right). \tag{4}$$

Clearly

$$|F(\theta)| \leqq 1 \tag{5}$$

for all θ and

$$F(0) = 1. \tag{6}$$

We choose ϱ, which is still at our disposal and may vary with n, so that the integrand in (3) has stationary phase in the neighbourhood of $\theta = 0$, that is so that

$$n = \sum_{b \in \mathfrak{B}} \frac{b\varrho^b}{1 + \varrho^b}. \tag{7}$$

This is possible since the right hand side of (7) increases continuously from 0 to ∞ as ϱ increases from 0 to $1-0$. The rest of this § 2 is devoted to showing that (3) holds provided that

$$n > \max \left\{ 2^{10M}, 2^{2^{2^{400}}} \right\}. \tag{8}$$

First we require an estimate of ϱ. It is convenient to work with the integer λ defined by the inequalities

$$\varrho^{2^\lambda} \geqq \frac{1}{2} > \varrho^{2^{\lambda+1}}. \tag{9}$$

From now on, n satisfies (8), and ϱ, λ are given by (7), (9) respectively.

Lemma 2.

$$\lambda \geqq \max \{8M, 2^{2^{300}}\}. \tag{10}$$

For, by (7) we have

$$n \leqq \sum_{b \in \mathfrak{B}} b\varrho^b \leqq \sum_{\substack{b \in \mathfrak{B} \\ b \leqq 2^M}} b + \sum_{m \geqq M} \sum_{\substack{2^m < b \leqq 2^{m+1} \\ b \in \mathfrak{B}}} b\varrho^b \leqq$$

$$\leqq 2^{2M} + \sum_{m \geqq 1} (2^{20} \log_2 m + 1) 2^{m+1} \varrho^{2^m} \leqq \frac{1}{2} n + \sum_{1 \leqq m \leqq \lambda} (2^{20} \log_2 m + 1) 2^{m+1} + \tag{11}$$

$$+ \sum_{m > \lambda} (2^{20} \log_2 m + 1) 2^{m+1} (1/2)^{2^{m-\lambda+1}} \leqq \frac{1}{2} n + (2^{20} \log_2 \lambda + 1) 2^{\lambda+5}.$$

The Lemma now follows from (8) and (11).

It is convenient to state for further reference two inequalities involving ϱ and λ. We do not give the proofs, which are all by a division of the range of summation as in the proof of Lemma 2.

Corollary. *The following estimates hold:*

$$\sum_{b\in\mathfrak{B}} b^3\varrho^b < 2^{3\lambda+30}\log_2\lambda, \tag{12}$$

$$\sum_{b\in\mathfrak{B}} \frac{b^2\varrho^b}{(1+\varrho^b)^2} < 2^{2\lambda+30}\log_2\lambda. \tag{13}$$

Lemma 3. *Let σ, Φ be real numbers such that*

$$\frac{1}{2} \leqq \sigma \leqq 1, \quad |\Phi| \leqq \pi. \tag{14}$$

Then

$$\left|\frac{1+\sigma e^{i\Phi}}{1+\sigma}\right|^2 \leqq \exp\{-4\Phi^2/9\pi^2\} \leqq 2^{-\Phi^2/2\pi^2}. \tag{15}$$

For

$$|1+\sigma e^{i\Phi}|^2 = (1+\sigma)^2 - 2\sigma\sin^2\Phi/2$$

and

$$|\sin\Phi/2| \geqq |\Phi|/\pi.$$

Hence

$$\left|\frac{1+\sigma e^{i\Phi}}{1+\sigma}\right|^2 \leqq 1-\frac{2\sigma}{(1+\sigma)^2}\frac{\Phi^2}{\pi^2} \leqq 1-4\Phi^2/9\pi^2 \leqq \exp\{-4\Phi^2/9\pi^2\}.$$

Corollary 1. *Suppose that*

$$2^{-N-1}\pi \leqq \theta \leqq (2-2^{-N-1})\pi. \tag{16}$$

Then

$$|F(\theta)| \leqq 2^{-2N-50}, \tag{17}$$

where $F(\theta)$ is given by (4).

For

$$|F(\theta)| \leqq \prod_{b\in\mathfrak{B},\, b\leqq 2^M} \left|\frac{1+\varrho^b e^{ib\theta}}{1+\varrho^b}\right|.$$

In each of the terms of the product we have

$$1 \geqq \varrho^b \geqq \varrho^{2^M} \geqq \varrho^{2^\lambda} \geqq \frac{1}{2}$$

by (9). Hence on applying Lemma 3 to each term, with

$$\sigma = \varrho^b \quad \text{and} \quad \Phi = \pm 2\pi\|b\theta/2\pi\|,$$

we have

$$|F(\theta)| \leqq 2^{-\Sigma \|b\theta/2\pi\|^2},$$

where the sum is over $b \in \mathfrak{B}$, $b \leqq 2^M$. The truth of (17) now follows from Lemma 1 (i).

For

$$N \leqq m < \lambda$$

we write

$$f_m(\theta) = \prod_{\substack{b \in \mathfrak{B} \\ 2^m < b \leqq 2^{m+1}}} \left(\frac{1 + \varrho^b e^{ib\theta}}{1 + \varrho^b} \right). \tag{18}$$

Corollary 2.

$$|f_{\lambda-1}(\theta)| \leqq \exp\{-2^{2\lambda+10} (\log_2 \lambda) \theta^2\} \tag{19}$$

for all θ in the range $|\theta| \leqq 2^{-\lambda}\pi$.

By Lemma 3 we have the estimate

$$|f_{\lambda-1}(\theta)|^2 \leqq \exp\left\{ \frac{-4}{9\pi^2} \sum_{\substack{b \in \mathfrak{B} \\ 2^{\lambda-1} < b \leqq 2^\lambda}} (b\theta)^2 \right\}.$$

Since there are at least $2^{20} \log_2 (\lambda - 1)$ summands, by Lemma 1 (ii), the required estimate follows.

Corollary 3. *Let*

$$\theta_0 = (\log_2 \lambda)^{-2/5} 2^{-\lambda} \pi. \tag{20}$$

Then

$$\int_{\theta_0}^{2^{-\lambda}\pi} |F(\theta)| d\theta \leqq 2^{-\lambda} (\log_2 \lambda)^{-1/2} \exp\{-2^{10} (\log_2 \lambda)^{1/5}\}. \tag{21}$$

For

$$|F(\theta)| \leqq |f_{\lambda-1}(\theta)| \tag{22}$$

and Corollary 3 follows from Corollary 2 with a little calculation.

Lemma 4. *Let σ, Φ, ψ be real numbers such that*

$$\frac{1}{2} \leqq \sigma \leqq 1, \quad \frac{\pi}{8} \leqq |\Phi - \psi| \leqq \pi. \tag{23}$$

Then

$$\left| \frac{1 + \sigma e^{i\Phi}}{1 + \sigma} \right| \left| \frac{1 + \sigma e^{i\psi}}{1 + \sigma} \right| \leqq 2^{-2^{-9}}. \tag{24}$$

Since

$$\frac{d}{d\Phi}\log|1+\sigma e^{i\Phi}|=\frac{-\sigma\sin\Phi}{1+\sigma^2+2\sigma\cos\Phi}$$

is monotone in $|\Phi|\leqq\pi/2$, it is easy to see that the left hand side of (26) attains its maximum when $\Phi=-\psi=\pi/16$ for fixed σ, when Φ,ψ are allowed to vary. Lemma 4 now follows from Lemma 3.

Corollary 1. *Let $N\leqq m<\lambda$ and let θ_0,θ_1 be two numbers such that*

$$2^{-m-3}\pi\leqq|\theta_0-\theta_1|\leqq 2^{-m-1}\pi. \tag{25}$$

Then

$$|f_m(\theta_0)f_m(\theta_1)|\leqq m^{-10}, \tag{26}$$

where $f_m(\theta)$ is defined in (18).

For, by Lemma 1 (ii),

$$|f_m(\theta_0)f_m(\theta_1)|=\prod_{\substack{2^m<b\leqq 2^{m+1}\\ b\in\mathfrak{B}}}\left|\frac{1+\varrho^b e^{ib\theta_0}}{1+\varrho^b}\right|\left|\frac{1+\varrho^b e^{ib\theta_1}}{1+\varrho^b}\right|$$

is the product of at least $2^{20}\log_2 m$ terms to each of which Lemma 4 applies.

Corollary 2. *Let $\mathfrak{I}$ be any interval of length*

$$|\mathfrak{I}|\leqq 2^{-m-1}\pi. \tag{27}$$

Then $\mathfrak{I}$ can be divided into 3 intervals $\mathfrak{K},\mathfrak{L},\mathfrak{M}$ each of length at most $2^{-m-2}\pi$, so that[1])

$$|f(\theta)|\leqq\frac{1}{4}m^{-4}\qquad(\theta\in\mathfrak{K},\mathfrak{L}). \tag{28}$$

We may suppose that $\mathfrak{I}$ is closed, so that $|f_m(\theta)|$ for $\theta\in\mathfrak{I}$ takes its maximum at some $\theta_0\in\mathfrak{I}$. If $|f_m(\theta_0)|\leqq\frac{1}{4}m^{-4}$, there is nothing to prove. If $|f_m(\theta_0)|>\frac{1}{4}m^{-4}$ we take for $\mathfrak{M}$ the points of $\mathfrak{I}$ for which $|\theta-\theta_0|\leqq 2^{-m-3}\pi$. By corollary 1 we have

$$|f_m(\theta)|\leqq m^{-10}/|f_m(\theta_0)|\leqq 4m^{-6}\leqq\frac{1}{4}m^{-4}$$

for $\theta\in\mathfrak{I},\theta\notin\mathfrak{M}$; and the result follows.

---

[1]) We do not exclude the possibility that one of the intervals is empty.

Lemma 5. *Let $\mathfrak{I}$ be any interval of length $|\mathfrak{I}| \leqq 2^{-\lambda}\pi$. Then*

$$\int_{\mathfrak{I}} |f_{\lambda-1}(\theta)|^{1/2} d\theta \leqq (\log_2 \lambda)^{-1/2} 2^{-\lambda}. \tag{29}$$

We use the rearrangement of functions as explained in HARDY, LITTLEWOOD and PÓLYA [5] Chapter X. If $u(\theta)$ is any continuous positive function defined for $\theta \in \mathfrak{I}$, then, just for this proof, we denote by $u^*(\theta)$ the symmetric rearrangement of $u(\theta)$; that is the unique function defined for $|\theta| \leqq \frac{1}{2}|\mathfrak{I}|$ by the following properties:

(A) $u^*(\theta)$ is continuous,

(B) $u^*(-\theta) = u^*(\theta)$,

(C) $u^*(\theta)$ decreases for $0 \leqq \theta \leqq \frac{1}{2}|\mathfrak{I}|$,

(D) for any number u_0, the set of θ in $|\theta| \leqq \frac{1}{2}|\mathfrak{I}|$ such that $u^*(\theta) > u_0$ has the same measure as the set of $\theta \in \mathfrak{I}$ such that $u(\theta) > u_0$.

If $u(\theta), v(\theta)$ are any two positive continuous functions defined in $\mathfrak{I}$ then it is easy to see that

$$\int_{\mathfrak{I}} u(\theta)v(\theta)d\theta \leqq \int_{|\theta| \leqq \frac{1}{2}|\mathfrak{I}|} u^*(\theta)v^*(\theta)d\theta). \tag{30}$$

(cf. HARDY, LITTLEWOOD and PÓLYA [5], Theorem 378).

In particular, when $\mathfrak{I}$ is as above and

$$u(\theta) = u_b(\theta) = \left| \frac{1 + \varrho^b e^{i\theta}}{1 + \varrho^b} \right|^{1/2}$$

for some integer b with $b \leqq 2^\lambda$, it is obvious that

$$u^*(\theta) \leqq u(\theta) \qquad \left(|\theta| \leqq \frac{1}{2}|\mathfrak{I}|\right).$$

Since

$$|f_{\lambda-1}(\theta)|^{1/2} = \prod_{\substack{b \in \mathfrak{B} \\ 2^{\lambda-1} < b \leqq 2^\lambda}} u_b(\theta),$$

repeated application of (30) gives

$$\int_{\mathfrak{I}} |f_{\lambda-1}(\theta)|^{1/2} d\theta \leqq \int_{|\theta| \leqq 2^{-\lambda-1}\pi} |f_{\lambda-1}(\theta)|^{1/2} d\theta \leqq \int_{-\infty < \theta < \infty} \exp\{-2^{2\lambda+9}(\log_2 \lambda)\theta^2\} d\theta,$$

by Lemma 3, Corollary 2.

Lemma 6. *Let m be any integer in $N \leqq m < \lambda$ and let $\mathfrak{I}$ be any interval of length $|\mathfrak{I}| \leqq 2^{-m-1}\pi$. Then*

$$S_m(\mathfrak{I}) \text{ (say)} = \int_{\mathfrak{I}} \Big| \prod_{m \leqq \mu < \lambda} f_\mu(\theta) \Big|^{1/2} d\theta < (\log_2 \lambda)^{-1/2} 2^{-\lambda} \prod_{m \leqq \mu < \lambda} (1 + \mu^{-2}).$$

When $m = \lambda - 1$, this is just Lemma 5. Otherwise we use backwards induction on m. Let $\mathfrak{K}, \mathfrak{L}, \mathfrak{M}$ be the intervals given by Lemma 4, Corollary 4. Then, in an obvious notation,

$$S_m(\mathfrak{I}) = S_m(\mathfrak{K}) + S_m(\mathfrak{L}) + S_m(\mathfrak{M}) \leqq$$

$$\leqq \frac{1}{2} m^{-2} S_{m+1}(\mathfrak{K}) + \frac{1}{2} m^{-2} S_{m+1}(\mathfrak{L}) + S_{m+1}(\mathfrak{M}),$$

since $|f_m(\theta)|^{1/2} \leqq \frac{1}{2} m^{-2}$ in $\mathfrak{K}, \mathfrak{L}$ and $|f_m(\theta)|^{1/2} \leqq 1$ in $\mathfrak{M}$. The intervals $\mathfrak{K}, \mathfrak{L}, \mathfrak{M}$ satisfy the condition of the Lemma with $m+1$ instead of m and the result follows.

Corollary. *Let $N \leqq m \leqq \lambda - 2$ and let $\mathfrak{I}^m$ be the interval*

$$2^{-\lambda}\pi \leqq \theta \leqq 2^{-m-1}\pi.$$

Then

$$S_m(\mathfrak{I}^m) \leqq (\log_2 \lambda)^{-1/2} 2^{-\lambda} \Big\{ \prod_{m \leqq \mu < \lambda} (1 + \mu^{-2}) - 1 \Big\}. \tag{31}$$

For $\mathfrak{I}^m$ is the union of $\mathfrak{I}^{m+1}$ and $\mathfrak{K}^{m+1}$, where $\mathfrak{K}^{m+1}$ is the interval

$$2^{-m-2}\pi < \theta \leqq 2^{-m-1}\pi.$$

By Lemma 4, Corollary 1, we have

$$|f_m(\theta)| \leqq m^{-10} < m^{-2}$$

for $\theta \in \mathfrak{K}^{m+1}$, since $f_m(0) = 0$. The required estimate now follows by induction on applying Lemma 6 with $m+1$ for m to the interval $\mathfrak{K}^{m+1}$ instead of $\mathfrak{I}$, and since

$$S_m(\mathfrak{I}^m) = S_m(\mathfrak{I}^{m+1}) + S_m(\mathfrak{K}^{m+1}) \leqq S_{m+1}(\mathfrak{I}^{m+1}) + m^{-2} S_m(\mathfrak{K}^{m+1}).$$

Lemma 7. *Let*

$$\theta_0 = (\log_2 \lambda)^{-2/5} 2^{-\lambda}\pi. \tag{32}$$

Then

$$\int_{\theta_0}^{2\pi - \theta_0} |F(\theta)| d\theta < 2^{-\lambda - 20} (\log_2 \lambda)^{-1/2}. \tag{33}$$

The integral in question is twice the integral over the range $\theta_0 \leqq \theta \leqq \pi$. We divide this into $2^{N+1}+1$ subintervals, namely

$\mathfrak{R}$: $\theta_0 \leqq \theta \leqq 2^{-\lambda}\pi$,

$\mathfrak{Q}$: $2^{-\lambda}\pi \leqq \theta \leqq 2^{-N-1}\pi$,

$\mathfrak{M}_j$: $j2^{-N-1}\pi \leqq \theta \leqq (j+1)2^{-N-1}\pi \qquad (1 \leqq j \leqq 2^{N+1})$.

Lemma 3, Corollary 3 gives at once

$$\int_{\mathfrak{R}} \leqq (\log_2 \lambda)^{-1/2} 2^{-\lambda} \exp\{-2^{10}(\log_2 \lambda)^{1/5}\} < 2^{-\lambda-25}(\log_2 \lambda)^{-1/2}, \tag{34}$$

by (10).

In the interval $\mathfrak{Q}$ we have, by (4) and (18),

$$|F(\theta)| \leqq \prod_{N \leqq \mu < \lambda} |f_\mu(\theta)| \leqq \prod_{N \leqq \mu < \lambda} |f_\mu(\theta)|^{1/2}.$$

Hence Lemma 6, Corollary with $m = N$ gives

$$\int_{\mathfrak{Q}} \leqq (\log_2 \lambda)^{-1/2} 2^{-\lambda} \{ \prod_{N \leqq \mu < \lambda} (1+\mu^{-2}) - 1 \} \leqq 2^{-\lambda-25}(\log_2 \lambda)^{-1/2}. \tag{35}$$

Finally, by Lemma 3, Corollary 1, in the intervals $\mathfrak{M}_j$ we have

$$F(\theta) \leqq 2^{-2N-50}$$

and so

$$|F(\theta)| \leqq 2^{-N-25}|F(\theta)|^{1/2} \leqq 2^{-N-25} \prod_{N \leqq \mu < \lambda} |f_\mu(\theta)|^{1/2}. \tag{36}$$

Hence by Lemma 6 with $m = N$ we have

$$\int_{\mathfrak{M}_j} \leqq 2^{-N-25}(\log_2 \lambda)^{-1/2} 2^{-\lambda} \prod_{N \leqq \mu < \lambda} (1+\mu^{-2}) \leqq 2^{-\lambda-N-24}(\log_2 \lambda)^{-1/2}. \tag{37}$$

The truth of the Lemma now follows at once from (34), (35) and (37).

Lemma 8. *Let*

$$\theta_0 = (\log_2 \lambda)^{-2/5} 2^{-\lambda}\pi. \tag{38}$$

Then

$$\Re \int_{-\theta_0}^{\theta_0} F(\theta) e^{-in\theta} d\theta > 2^{-\lambda-20}(\log_2 \lambda)^{-1/2}. \tag{39}$$

Write

$$v_b(\theta) = \log\left\{ \frac{1+\varrho^b e^{ib\theta}}{1+\varrho^b} \right\}. \tag{40}$$

Then

$$v_b'''(\theta) = \frac{-\varrho^b(1-\varrho^b e^{ib\theta})b^3}{(1+\varrho^b e^{ib\theta})^3}.$$

If now

$$|\theta| \leqq \theta_0,$$

one readily obtains the estimate

$$|v_b'''(\theta)| \leqq 6\varrho^b b^3, \tag{41}$$

on considering separately the two cases

$$b \geqq 2^{\lambda+1}, \quad \text{so} \quad \varrho^b < \frac{1}{2}$$

and

$$b < 2^{\lambda+1}, \quad \text{so} \quad |b\theta| \leqq 2\pi(\log_2\lambda)^{-2/5} \leqq \pi/4,$$

by Lemma 2. Hence, using TAYLOR's theorem with remainder, we have

$$\left|\log\left(\frac{1+\varrho^b e^{ib\theta}}{1+\varrho^b}\right) - \frac{i\varrho^b b\theta}{1+\varrho^b} + \frac{\varrho^b(b\theta)^2}{2(1+\varrho^b)^2}\right| \leqq \varrho^b|b\theta|^3 \leqq \varrho^b(b\theta_0)^3. \tag{42}$$

Summing over $b \in \mathfrak{B}$ and recollecting that ϱ was chosen so that

$$n = \sum_{b\in\mathfrak{B}} \frac{b\varrho^b}{1+\varrho^b}$$

we have

$$|\log\{F(\theta)e^{-in\theta}\} + \tau\theta^2| \leqq \sum_{b\in\mathfrak{B}} \varrho^b(b\theta_0)^3, \tag{43}$$

where

$$2\tau = \sum_{b\in\mathfrak{B}} \frac{b^2\varrho^b}{(1+\varrho^b)^2}. \tag{44}$$

The sums occurring here were estimated in Lemma 2, Corollary. In the first place,

$$\Sigma\varrho^b(b\theta_0)^3 \leqq 2^{3\lambda+30}(\log_2\lambda)\theta_0^3 \leqq \pi^3 2^{30}(\log_2\lambda)^{-1/5} < 2^{-4} \tag{45}$$

by Lemma 2. Further, by Lemma 2, Corollary and (44),

$$2\tau < 2^{2\lambda+30}\log_2\lambda = 2\tau_2 \text{ (say)}. \tag{46}$$

By (43), (45), (46) it follows that

$$\Re\int_{-\theta_0}^{\theta_0} F(\theta)e^{-in\theta}d\theta \geqq \frac{1}{2}\int_{-\theta_0}^{\theta_0}\exp\{-\tau\theta^2\}d\theta \geqq \frac{1}{2}\int_{-\theta_0}^{\theta_0}\exp\{-\tau_0\theta^2\}d\theta \geqq \frac{1}{4}\tau_0^{-1/2}, \tag{47}$$

since $\tau_0\theta_0^2 > 1$ by (38) and (46).

The truth of the Lemma now follows from (46) and (47).

We note now that Lemmas 7, 8 together show that

$$\Re \int_{-\pi}^{\pi} F(\theta) e^{-in\theta} d\theta > 0.$$

This implies (3), and so the truth of the Theorem, as was remarked in the discussion that led up to (3).

3. Proof of Theorem II

Let α be any irrational number with bounded partial quotients and let $\varepsilon > 0$ be arbitrarily small. We consider first the set $\mathfrak{D}$ of positive integers

$$d_1 < d_2 < \cdots$$

such that

$$\|d\alpha\| < d^{-\frac{1}{2}(1+\varepsilon)}.$$

Lemma 9. *There are numbers $\gamma_1 > 0, \gamma_2$ depending only on α and ε, such that*

$$\gamma_1 < \frac{d_{j+1} - d_j}{d_j^{\frac{1}{2}(1+\varepsilon)}} < \gamma_2,$$

for all sufficiently large j.

We have

$$\|(d_{j+1} - d_j)\alpha\| \leqq \|d_{j+1}\alpha\| + \|d_j\alpha\| < 2d_j^{-\frac{1}{2}(1+\varepsilon)}.$$

This gives the left-hand inequality, since α has bounded partial quotients. (See, for example, CASSELS [3], Chapter I.)

Now let d_j be given and let $p'/q', p''/q'', p'''/q'''$ be the three consecutive best approximations to α such that

$$q' \leqq 4d_j^{\frac{1}{2}(1+\varepsilon)} < q'' < q'''.$$

Then

$$q' < q''' < \gamma_3 d_j^{\frac{1}{2}(1+\varepsilon)},$$

where γ_3 depends only on α, and

$$\|q''\alpha\| = |q''\alpha - p''| < p''^{-1} < \frac{1}{4} d_j^{-\frac{1}{2}(1+\varepsilon)}, \quad \|q'''\alpha\| = |q'''\alpha - q'''| < \frac{1}{4} d_j^{-\frac{1}{2}(1+\varepsilon)}.$$

Further, $(q''\alpha - p'')$ and $(q'''\alpha - p''')$ have opposite signs, so

$$\min\{\|(d_j + q'')\alpha\|, \|(d_j + q''')\alpha\|\} \leqq \frac{3}{4} d_j^{-\frac{1}{2}(1+\varepsilon)}.$$

Hence at least one of the two numbers d_j+q'' and d_j+q''' lies in $\mathfrak{D}$ provided that d_j is large enough. This proves the right-hand inequality.

Corollary 1.

$$\lim_{j\to\infty}\frac{d_{j+1}-d_j}{d_j^{1/2+\varepsilon}}=0. \tag{48}$$

Corollary 2.

$$\sum_{d\in\mathfrak{D}}\|d\alpha\|<\infty. \tag{49}$$

Corollary 1 is immediate. To prove Corollary 2, we note that, by Lemma 9, there are $O\left(2^{\frac{1}{2}j(1+\varepsilon)}\right)$ elements $d\in\mathfrak{D}$ in $2^j<d\leqq 2^{j+1}$. Hence the contribution of the terms with $2^j<d\leqq 2^{j+1}$ to the sum in (49) is $O\left(2^{-\frac{1}{2}j\varepsilon}\right)$. Since $\sum_j 2^{-\frac{1}{2}j\varepsilon}<\infty$, the result follows.

We also consider the set $\mathfrak{T}$ of integers $t>0$ such that

$$\|t\alpha\|<\frac{1}{4}\varepsilon.$$

Since α is irrational, the fractional parts of $n\alpha$ $(n=1,2,3,\ldots)$ are uniformly distributed, and hence

$$\lim_{n\to\infty}n^{-1}T(n)=\frac{1}{2}\varepsilon$$

(see, for example, CASSELS [3], Chapter IV).

Hence, and by Lemma 9, Corollary 2, there exists an integer N such that

$$T(n)<\varepsilon n \qquad (\text{for all } n\geqq N) \tag{50}$$

and

$$\sum_{d\in\mathfrak{D},\,d\geqq N}\|d\alpha\|<\frac{1}{4}\varepsilon.$$

Denote by $\mathfrak{C}$ the set of elements c of $\mathfrak{D}$ with $c\geqq N$. If s is the sum of distinct elements of $\mathfrak{C}$, we have clearly

$$s\geqq N \tag{51}$$

and

$$\|s\alpha\|\leqq\sum_{c\in\mathfrak{C}}\|c\alpha\|<\frac{1}{4}\varepsilon,$$

that is,

$$s\in\mathfrak{T}. \tag{52}$$

The set $\mathfrak{C}$ has the property (i) of the enunciation of Theorem II by Lemma 9, Corollary 1, and it has property (iii) by (50), (51) and (52). It remains only to show that $\mathfrak{C}$ contains infinitely many elements in every arithmetic progression, say in $lu+v$ $(l=0, 1, 2, \ldots)$, where $u>0$, $v>0$ are fixed integers. That is, we must show that there exist infinitely many integers l such that

$$lu+v \geqq N,$$

$$\|(lu+v)\alpha\| \leqq (lu+v)^{-\frac{1}{2}(1+\varepsilon)}. \tag{53}$$

But now an old theorem of KHINTCHINE [6] states that if θ is irrational and β is any real number, then

$$\liminf_{l\to\infty} l\|l\theta+\beta\| \leqq 5^{-1/2}. \tag{54}$$

This theorem with $\theta=u\alpha$, $\beta=v\alpha$ certainly implies the existence of infinitely many solutions of (53). (For a short proof of a slightly stronger form of KHINTCHINE's theorem see CASSELS [2]. For the latest in this direction see DESCOMBES [4].)

References

[1] B. J. BIRCH, On a problem of Erdős, *Proceedings Cambridge Phil. Soc.*, **55** (1959), 370—373.
[2] J. W. S. CASSELS, The lattice properties of asymmetric hyperbolic regions. I. On a theorem of Khintchine, *Proceedings Cambridge Phil. Soc.*, **44** (1948), 1—7.
[3] J. W. S. CASSELS, *An introduction to Diophantine approximation*, Cambridge Tract N° 45 (Cambridge, 1957).
[4] R. DESCOMBES, Sur la répartition des sommets d'une ligne polygonale régulière non fermée, *Annales École Normale Supérieure*, **73** (1956), 283—355.
[5] G. H. HARDY, J. E. LITTLEWOOD and G. PÓLYA, *Inequalities* (Cambridge, 1934).
[6] A. KHINTCHINE, Neuer Beweis und Verallgemeinerung eines Hurwitzschen Satzes, *Math. Annalen*, **111** (1935), 631—637.
[7] K. F. ROTH—G. SZEKERES, Some asymptotic formulae in the theory of partitions, *Quarterly J. Math.*, **5** (1954), 241—259.

TRINITY COLLEGE
CAMBRIDGE

(Received September 3, 1959)

Semigroups in which every proper subideal is a group

By ŠTEFAN SCHWARZ in Bratislava (ČSR)

To Professor L. Rédei on the occasion of his sixtieth birthday

Let S be a semigroup. A left ideal of S is a non-vacuous subset $L \subset S$ for which $SL \subset L$ holds. A right ideal is a subset $R \subset S$ with $RS \subset R$. A subset which is both a left and right ideal of S is called a two-sided ideal of S.

If L_1, L_2 are left ideals of S, their union $L_1 \cup L_2$ and their intersection $L_1 \cap L_2$, if it is non-vacuous, is again a left ideal of S. A left ideal L of S is called a minimal left ideal of S if there does not exist a left ideal L' of S such that $L' \subsetneq L$ holds. The intersection of two minimal left ideals is the empty set. Analogous statements hold for right ideals.

Every semigroup which is not a group contains at least one left or right proper subideal.

Definition. A semigroup S is called to be an *F-semigroup* if it is not a group, but every left and right proper subideal of S is a group.

The purpose of this paper is to describe the structure of all F-semigroups. This is a generalization of a problem treated by POLLÁK and RÉDEI [4] who dealt with semigroups in which every proper subsemigroup is a group.

In section 1 we prove some preliminary lemmas needed in the following. In section 2 we describe the construction of two classes of semigroups that will turn out to be F-semigroups. Section 3 is devoted to the proof of the main Theorem 1. In section 4 we show that the result of [4] is a simple consequence of Theorem 1.

1.

Lemma 1. *Let L be a left ideal of the semigroup S and G a group contained in S. If $L \cap G \neq \emptyset$, then $G \subset L$.*

Proof. Let be $a \in L \cap G$. Then $G = Ga \subset SL \subset L$, q. e. d.

An analogous result holds for right ideals.

Every F-semigroup contains at least one minimal left ideal. For, if S does not contain any proper left subideal of S, then the semigroup S is itself a minimal left ideal of S. If S contains a proper left subideal $L \subsetneqq S$, then, by supposition, L is a group and since a group cannot contain as a proper subset an ideal of S, L is a minimal left ideal of S.

Lemma 2. *Let S be an F-semigroup. Then only one of the following cases can occur:*

A) *either S has a unique minimal proper left subideal;*

B) *or S contains precisely two different minimal left ideals $L_1 \subsetneqq S$, $L_2 \subsetneqq S$ and $S = L_1 \cup L_2$ holds;*

C) *or S does not contain any left ideal $\neq S$ at all.*

Proof. S cannot contain more then two distinct minimal left ideals. For, if there were at least three distinct minimal left ideals, say L_1, L_2, L_3, we would have $S \supset L_1 \cup L_2 \cup L_3 \supsetneqq L_1 \cup L_2 \supsetneqq L_1$. But then $L_1 \cup L_2$ would be a proper subideal of S, which is not a group.

If S contains two different minimal left ideals, say L_1 and L_2, then $S \supset L_1 \cup L_2 \supsetneqq L_1$ implies $S = L_1 \cup L_2$. This proves our Lemma.

Remark 1. We shall see that each of these possibilities really occurs.

Remark 2. Needless to say that an analogous result holds for minimal right ideals.

We recall the following well known fact:

Lemma 3. *If L is a minimal left ideal of a semigroup S and $a \in S$, then La is also a minimal left ideal of S.*

Proof. Suppose that K is a left ideal of S with $K \subset La$. Let be $L_1 = \{x | x \in L, xa \in K\}$. If $z \in S$, we have $zxa \in K$ so that $zx \in L_1$. Hence L_1 is a left ideal. Since L is minimal, we have $L_1 = L$, hence $La = K$, and La has no proper left subideal.

A left ideal L is called to be maximal if there is no left ideal L' such that $L \subsetneqq L' \subsetneqq S$. Maximal right and two-sided ideals are defined analogously.

The following lemma will be useful:

Lemma 4. *Let M be a maximal two-sided ideal of S which is not contained as a proper subset in a left or right ideal of S and different from S. Then*

a) *either $S - M$ is a group;*

b) *or $S - M$ contains a unique element u, with $u^2 \in M$.*

Remark. Analogous theorems have been proved in the paper [6].

Proof. a) Suppose first that $S-M$ contains at least two elements. Denote $S-M=G$ and choose an element $a\in G$. The left ideal $M\cup\{a\}\cup Sa$ contains M and a, hence $M\cup\{a\}\cup Sa=S$. Since $S-M$ contains more than one element the left ideal $M\cup Sa$ contains M as a proper subset, hence we have also $M\cup Sa=S$. If $x\in M$, we have $M\cup Sx\subset M\cup SM\subset M$. Therefore the set G is characterized by the property that $G=\{x|x\in S, M\cup Sx=S\}$.

We show first that G is a semigroup. To this end it is sufficient to prove: If $M\cup Sa=S$, $M\cup Sb=S$, then we have also $M\cup Sab=S$. This follows in the following manner: Multiplying the first relation by b we get $Mb\cup Sab=Sb$. Hence $M\cup Mb\cup Sab=M\cup Sb$, i. e. $M\cup Sab=S$.

The relation $M\cup Sa=S$ (which is true for every $a\in G$) can be written in the following manner: $M\cup[M\cup G]a=M\cup G$, i. e. $M\cup Ga=M\cup G$. Since $M\cap G=\emptyset$, we have $Ga\supset G$. On the other side G is a semigroup, hence $Ga\subset G^2\subset G$. Therefore $Ga=G$. Analogously we can prove $aG=G$. The equations $Ga=G$, $aG=G$ for every $a\in G$ imply that G is a group.

b) Suppose next that $S-M$ contains a unique element, $S-M=\{u\}$. If u is an idempotent, $\{u\}$ forms itself a group. If u is not an idempotent, we have necessarily $u^2\in S-\{u\}=M$. This proves Lemma 4.

2.

In this section we deal with the construction of two types of semigroups that will be needed in section 3. Analogous constructions (in entirely other connections) have been studied previously by CLIFFORD [1], HEWITT [2] and HEWITT—ZUCKERMAN [3].

Lemma 5. *Let G_1 and G_0 be two disjoint groups. Let φ_{10} be a homomorphic mapping of the group G_1 into the group G_0. Let further φ_{00} and φ_{11} denote the identical automorphisms of the groups G_0, G_1, respectively. Consider the set $S=G_0\cup G_1$ in which we introduce a multiplication $\odot$ by the following definition: If $a_i\in G_i$, $b_j\in G_j$ $(i,j=0,1)$ let be:*

$$a_i\odot b_j=\varphi_{i,ij}(a_i)\varphi_{j,ij}(b_j). \tag{1}$$

Then S is a semigroup with the unit element equal to the unit element of the group G_1.

Remark. The multiplication is defined in such a manner that inside the groups G_0, G_1 it is identical with the original multiplication in these groups. If namely $i=j=1$, i. e. $a_1\in G_1$, $b_1\in G_1$, $a_1\odot b_1=\varphi_{11}(a_1)\varphi_{11}(b_1)=a_1b_1$. If $i=k=0$, i. e. $a_0\in G_0$, $b_0\in G_0$, we have $a_0\odot b_0=\varphi_{00}(a_0)\varphi_{00}(b_0)=a_0b_0$.

Proof. a) For $i \geqq j \geqq k$ $(i, j, k = 0, 1)$ we have clearly

$$\varphi_{ik} = \varphi_{jk}\, \varphi_{ij}. \tag{2}$$

b) Let be $a_i \in G_i$, $b_j \in G_j$, $c_k \in G_k$ $(i, j, k = 0, 1)$. Then we have

$$(a_i \odot b_j) \odot c_k = [\varphi_{i,ij}(a_i)\varphi_{j,ij}(b_j)] \odot c_k.$$

Since the expression in the bracket on the right hand side is contained in the group G_{ij} we can further write

$$(a_i \odot b_j) \odot c_k = \varphi_{ij,ijk}[\varphi_{i,ij}(a_i)\varphi_{j,ij}(b_j)] \cdot \varphi_{k,ijk}(c_k).$$

Since $ij \geqq ijk$ $\varphi_{ij,ijk}$ is one of our three mappings φ_{11}, φ_{10}, φ_{00}. Further, according to (2) we have

$$\varphi_{ij,ijk}\, \varphi_{i,ij} = \varphi_{i,ijk}, \quad \varphi_{ij,ijk}\, \varphi_{j,ij} = \varphi_{j,ijk}.$$

Therefore

$$(a_i \odot b_j) \odot c_k = [\varphi_{i,ijk}(a_i)\varphi_{j,ijk}(b_j)]\varphi_{k,ijk}(c_k). \tag{3}$$

Analogously we prove

$$a_i \odot (b_j \odot c_k) = \varphi_{i,ijk}(a_i)[\varphi_{j,ijk}(b_j)\varphi_{k,ijk}(c_k)]. \tag{4}$$

Since each of the factors on the right hand side of the equations (3) and (4) is contained in the group G_{ijk}, and the multiplication in this group is associative, we have really $(a_i \odot b_j) \odot c_k = a_i \odot (b_j \odot c_k)$, i. e. S is a semigroup.

c) If e_1 is the unit element of the group G_1, we have for $b_k \in G_k$ (according to (1))

$$e_1 \odot b_k = \varphi_{1,k}(e_1)\varphi_{kk}(b_k) = \varphi_{1,k}(e_1) b_k.$$

For $k = 1$ we have $e_1 \odot b_1 = \varphi_{11}(e_1) b_1 = e_1 b_1 = b_1$. For $k = 0$ (since $\varphi_{10}(e_1) = e_0$) we have $e_1 \odot b_0 = \varphi_{10}(e_1) b_0 = e_0 b_0 = b_0$. Hence $e_1 \odot b_k = b_k$. Analogously we can prove $b_k \odot e_1 = b_k$, i. e. e_1 is the unit element of the semigroup S. This proves our lemma.

Definition. The semigroup S obtained by means of the construction from Lemma 5 will be denoted by $S = S[G_1, G_0; \varphi_{10}]$.

The notation is chosen to emphasize the means needed for the construction of S.

Corollary 5. *In the semigroup* $S[G_1, G_0; \varphi_{10}]$ *the homomorphism* φ_{10} *is uniquely determined by the relation: For* $a \in G_1$ *we have* $\varphi_{10}(a) = a \odot e_0$.

Proof. For $a_1 \in G_1$ we have [by (1)]

$$a_1 \odot e_0 = \varphi_{10}(a_1)\varphi_{00}(e_0) = \varphi_{10}(a_1) e_0.$$

Since $\varphi_{10}(a_1) \in G_0$, we have $a_1 \odot e_0 = \varphi_{10}(a_1)$, q. e. d.

Lemma 6. *Every semigroup of the type* $S[G_1, G_0; \varphi_{10}]$ *is an F-semigroup in which* G_0 *is the unique proper two-sided subideal.*

Proof. First, it is clear that G_0 is a two-sided subideal of S which being a group cannot contain as a proper subset a subideal of S. Next, any ideal which contains an element $\in G_1$ contains the whole group G_1, hence it contains also e_1 and it is equal to S. Therefore our semigroup contains a unique proper subideal which is a group.

Lemma 7. *Let* G *a group and* u *an element non* $\in G$. *Let* b *be a fixed chosen element,* $b \in G$. *Consider the set* $S = G \cup \{u\}$ *with the multiplication* $\odot$ *defined as follows:*

a) *for* $x, y \in G$ *let be* $x \odot y = xy$;

b) $u \odot u = b^2$;

c) *for* $x \in G$ *let be* $u \odot x = bx$ *and* $x \odot u = xb$. *Then* S *is a semigroup.*

Proof. Let be $\xi \in S$. Define

$$\bar{\xi} = \begin{cases} \xi & \text{for } \xi \in G, \\ b & \text{for } \xi = u. \end{cases}$$

In both cases we have $\bar{\xi} \in G$. For every couple $\xi, \eta \in S$ we have clearly $\xi \odot \eta = \bar{\xi}\bar{\eta}$. Therefore for arbitrary three elements $\xi, \eta, \zeta \in S$ we have

$$\xi \odot (\eta \odot \zeta) = \bar{\xi}(\overline{\eta\zeta}) = \bar{\xi}(\bar{\eta}\bar{\zeta}) = (\bar{\xi}\bar{\eta})\bar{\zeta} = (\overline{\xi\eta})\bar{\zeta} = (\xi \odot \eta) \odot \zeta.$$

Hence S is a semigroup.

Definition. The semigroup constructed in Lemma 7 will be denoted by $S = S[G, u; b]$.

Corollary 7. *In the semigroup* $S[G, u; b]$ *the element* b *is uniquely determined by the equation* $b = u \odot e = e \odot u$, *where* e *is the unit element of the group* G.

Proof. Puting $x = e$ we get [according to c)] $u \odot e = be, e \odot u = eb$. But since $b \in G$, we have $eb = be = b$; hence $b = u \odot e = e \odot u$.

Lemma 8. *Every semigroup of the type* $S[G, u; b]$ *is an F-semigroup. Its unique proper (two-sided) ideal is the group* G.

Proof. Clearly, G is a two-sided ideal of S. Since G is a group, it is at the same time the minimal two-sided ideal of S. Every ideal I of S different from S must contain the element u. But then we have also $u^2 \in I$, hence $G \cap I \neq \emptyset$. By Lemma 1, we have then necessarily $G \subset I$, hence $S = G \cup \{u\} \subset I$, i. e. $S = I$. Hence G is the unique proper subideal of S.

Remark. If we choose in Lemma 7 for b different elements $\in G$ the semigroups thus obtained need not be isomorphic. This can be shown on simple examples. Let G be the group of second order $G=\{e, a\}$ and choose first $b=e$. Then $S_1=S_1[G, u; e]$ has the following multiplication table:

	e	a	u
e	e	a	e
a	a	e	a
u	e	a	e

Choose next in the same group $b=a$. Then $S_2=S_2[G, u; a]$ has the multiplication table:

	e	a	u
e	e	a	a
a	a	e	e
u	a	e	e

The semigroups S_1 and S_2 are neither isomorphic nor antiisomorphic.

3.

The following theorem gives a solution of the problem mentioned in the introduction.

Theorem 1. *A semigroup is an F-semigroup if and only if it is isomorphic with a semigroup belonging to one of the following classes of semigroups:*

a) *the class of semigroups of the type* $S[G_1, G_0; \varphi_{10}]$ *(see Lemma 5);*

b) *the class of semigroups of the type* $S[G, u; b]$ *(see Lemma 7);*

c) *the class of semigroups of the form* $G\times H$, *where* G *is a group and* $H=\{e_1, e_2\}$ *is a semigroup in which* $e_i e_k = e_i$ $(i, k=1, 2)$;

d) *the class of semigroups of the form* $G\times H'$, *where* G *is a group and* $H'=\{e_1, e_2\}$ *is a semigroup in which* $e_i e_k = e_k$ $(i, k=1, 2)$.

Proof. According to Lemma 2 we have to consider three cases A, B, C.

Case A. Let S be an F-semigroup and suppose that it has a unique minimal proper left subideal L.

Let be $a\in S$. Since La is a minimal left ideal of S (see Lemma 3), we have $La=L$, i. e. $LS=L$; hence L is a two-sided ideal of S. The ideal L cannot be contained in a left (right) ideal L' of S such that $L\subsetneqq L'\subsetneqq S$ holds. For, the ideal L' would be a group and since $\emptyset\neq L\subset L'\cap L$ Lemma 1 would imply $L'\subset L$, i.e. $L'=L$, which is a contradiction. Hence L is a

maximal two-sided ideal of S which is not properly contained in a left or right ideal of S different from S.

By Lemma 4, there are two possibilities which are necessary to investigate separately.

a) Let $S-L=G_1$ be a group. Then $S=L\cup G_1$ is a union of two disjoint groups.

Let e_0 and e_1 be the unit elements of the groups L and G_1. If $a\in G_1$, we have $ae_0\in aL=L$. The mapping

$$\psi_{10}:\ a\in G_1\to ae_0\in L \tag{5}$$

is a homomorphic mapping of the group G_1 into the group L. If namely $a\in G_1$, $b\in G_1$ and $a\to ae_0$, $b\to be_0$, we have $ab\to abe_0=a(be_0)=a[e_0(be_0)]=$ $=(ae_0)(be_0)$.

If further $a\in G_1$, $b\in L$, we have

$$ab=a(e_0b)=(ae_0)b=\psi_{10}(a)b,$$
$$ba=(be_0)a=b(e_0a)=[b(e_0a)]e_0=(be_0)(ae_0)=b(ae_0)=b\psi_{10}(a).$$

Put — for a while — $L=G_0$ and denote by ψ_{00} and ψ_{11} the identical automorphisms of the groups $L=G_0$ and G_1. We then have for $a_i\in G_i$ and $b_j\in G_j$

$$a_ib_j=\psi_{i,ij}(a_i)\psi_{j,ij}(b_j).$$

Hence, in the notations of Lemma 5, we have necessarily $S=S[G_1,L;\psi_{10}]$. Hereby, in accordance with Corollary 5, ψ_{10} is defined by the relation (5).

Conversely, we know from Lemma 6 that $S[G_1,L;\psi_{10}]$ is an F-semigroup.

b) Let $S-L=\{u\}$, where $u^2\in L$. Denote by e the unit element of the group L. Denote further $b=ue$.

Since $b\in uL\subset L$, we have $b=eb=eue$. Since $eu\in Lu=L$ we have $(eu)e=eu$. Hence we have also $b=eu$.

Further $u^2\in L$ implies $u^2=eu^2e=(eu)(ue)=b^2$.

Finally for $x\in L$ we have $ux=u(ex)=(ue)x=bx$ and $xu=(xe)u=$ $=x(eu)=xb$. Our semigroup is necessarily of the type $S[G,u;b]$, where, in accordance with Corollary 7, we have $b=ue$.

Conversely, we know (see Lemma 8) that every semigroup of the type $S[G,u;b]$ is an F-semigroup.

Case B. Let S be an F-semigroup. Suppose that it contains precisely two minimal left ideals L_1, L_2. Then, by Lemma 2, we have necessarily $S=L_1\cup L_2$. Denote by e_1, e_2 the unit elements of the groups L_1 and L_2.

We show first that S cannot contain a proper right subideal $R \neq S$. If R is a right ideal of S, we have $\emptyset \neq RL_1 \subset R \cap L_1$. Since the group L_1 has a non-empty intersection with the right ideal R, we have (by Lemma 1) $L_1 \subset R$. Analogously $L_2 \subset R$. Hence $S = L_1 \cup L_2 \subset R$, i. e. $S = R$.

S is therefore a so called right simple semigroup containing idempotents.

It is known (see f. i. [5]) that in every right simple semigroup T containing idempotents every idempotent is a left unit and the semigroup itself is a union of disjoint isomorphic groups. The set of left units $H \subset T$ forms clearly a subsemigroup of T. Further it is known that the semigroup T is isomorphic to the direct product $G \times H$, where G is a group (namely the abstract group isomorphic to the groups whose union is T itself).

In our case the right simple semigroup S contains two idempotents e_1, e_2, hence we have necessarily $S \cong G \times H$, where G is a group and $H = \{e_1, e_2\}$ has the multiplication table

	e_1	e_2
e_1	e_1	e_2
e_2	e_1	e_2 .

(6)

The left ideals L_1, L_2 of S are then isomorphic to the group G.

Conversely, if G is an arbitrary group and H a semigroup with the multiplication table (6), then $G \times H$ is a semigroup without a proper right subideal. It contains precisely two proper left subideals, namely $G \times \{e_1\}$ and $G \times \{e_2\}$, both being groups (and both isomorphic to G). Hence $G \times H$ is an F-semigroup.

Case C. Suppose that S is an F-semigroup which does not contain a proper left subideal. Hence $Sa = S$ for every $a \in S$.

Let R be a minimal right ideal of S. The set $SR = \bigcup_{a_\nu \in S} a_\nu R$ is a two-sided ideal of S, hence $SR = S$. Since, by Lemma 3, every summand $a_\nu R$ is a minimal right ideal of S, we conclude that S is the union of its minimal right ideals. By Lemma 2 (formulated for right ideals) we conclude further that a) either S does not contain a proper right subideal at all, b) or S is the sum of two minimal right ideals of S (each of which is a group).

a) The case that S does not contain a proper right subideal is impossible. For then we would have also $aS = S$ for every $a \in S$. The relations $Sa = S$, $aS = S$ for every $a \in S$ imply that S is a group, contrary to the supposition that S is an F-semigroup.

b) In the second case, if $S = R_1 \cup R_2$, and R_1, R_2 are two different minimal right ideals of S, we can use the result proved sub B by inter-

changing the role of left and right ideals. If e_1, e_2 are the unit elements of the groups R_1, R_2, we conclude that the semigroup is necessarily isomorphic to the direct product $G \times H'$, where G is a group and H' is a semigroup with the multiplication table

	e_1	e_2
e_1	e_1	e_1
e_2	e_2	e_2

(7)

Conversely, every semigroup of the type $G \times H'$, where G is a group and H' is a semigroup with the multiplication table (7), is an F-semigroup without proper left subideals, containing precisely two proper right subideals each of which is a group.

This completes the proof of Theorem 1.

4.

In this section we show that the result of paper [4] is an immediate consequence of Theorem 1.

We shall use the following notations.

Let S be a semigroup and $a \in S$. The cyclic subsemigroup of S generated by a will be denoted by $[a]$. An element $a \in S$ is called to be of finite order if $[a]$ is contains only a finite number of different elements. If every element of S is of finite order, S is called a torsion semigroup. If a is of finite order, $[a]$ is called to be of the type (m, n), if n is the least integer such that there is an integer $m < n$ with $a^m = a^{n+1}$. If $[a]$ is of the type (m, n), $[a]$ contains exactly n different elements and it is well known that $\{a^m, a^{m+1}, \ldots, a^n\}$ is the greatest group contained in $[a]$.

Definition. A semigroup S is called to be an E-semigroup if every proper subsemigroup of S is a group.

Theorem 2 (Pollák—Rédei [4]). *A semigroup is an E-semigroup if and only if S belongs to one of the following types of semigroups:*

a) *S is a torsion group;*

b) *S is a cyclic semigroup $[a]$ of the type $(2, n)$, where $n > 2$ is an integer;*

c) *$S = \{e_1, e_0\}$, where $e_0^2 = e_0 e_1 = e_1 e_0 = e_0$, $e_1^2 = e_1$;*

d) *$S = \{e_1, e_2\}$, where $e_i e_k = e_i$ for $i, k = 1, 2$;*

e) *$S = \{e_1, e_2\}$, where $e_i e_k = e_k$ for $i, k = 1, 2$.*

Proof. An E-semigroup is clearly a torsion semigroup. For if there were an $a \in S$ which is not of finite order, then $[a] = \{a, a^2, \ldots\}$ would contain the subsemigroup $\{a^2, a^3, \ldots\}$ which is not a group.

An E-semigroup is necessarily either a group or an F-semigroup. Since a torsion group is clearly an E-semigroup, we have only to discuss the four cases of Theorem 1.

a) Let $S = S[G_1, G_0; \varphi_{10}]$ and suppose that S is an E-semigroup. Let e_1, e_0 be the unit elements of the groups G_1 and G_0. The two-element set $T_1 = \{e_1, e_0\} \subset S$ with the multiplication table

	e_1	e_0
e_1	e_1	e_0
e_0	e_0	e_0

forms a semigroup which is not a group. Hence $S = T_1$. Conversely, T_1 is clearly an E-semigroup.

b) Let $S = S[G, u; b]$ and suppose that S is an E-semigroup. Consider the cyclic semigroup $[u] \subset S$. Since $[u]$ is not a group (i. e. it is not of the type $(1, n)$), we have necessarily $[u] = S$. If $[u]$ were of the type (m, n) with $m \geqq 3$ the semigroup $\{u^2, u^3, \ldots u^n\} \subsetneq [u]$ would be a proper subsemigroup of S which is not a group. It remains the case that $[u]$ is of the type $(2, n)$. Conversely, in this case S is obviously an E-semigroup.

c) Let be $S \cong G \times H$. Denote by e the unit element of the group G. The semigroup $\{e\} \times H$ is a subsemigroup of $G \times H$ which is not a group. Hence $S \cong \{e\} \times H$. But $\{e\} \times H \cong H$, thus $S \cong H$. Conversely, H is obviously an E-semigroup.

d) The case $S \cong G \times H'$ can be settled analogously. This completes the proof of Theorem 2.

References

[1] A. H. Clifford, Semigroups admitting relative inverses, *Annals of Math.*, **42** (1941), 1037—1049.

[2] E. Hewitt, Compact monothetic semigroups, *Duke Math. Journal*, **23** (1956), 447—458.

[3] E. Hewitt—S. H. Zuckerman, Finite dimensional convolution algebras, *Acta Mathematica*, **93** (1955), 67—119.

[4] G. Polák—L. Rédei, Die Halbgruppen, deren alle echte Teilhalbgruppen Gruppen sind, *Publicationes Math. Debrecen*, **6** (1959), 126—130.

[5] Š. Schwarz, The structure of simple semigroups without zero, *Czechoslovak Math. Journal*, **1 (76)** (1951), 41—53.

[6] Š. Schwarz, Maksimaljnyje idealy v teorii polugrupp. II, *Czechoslovak Math. Journal*, **3 (78)** (1953), 365—383.

(Received September 5, 1959)

A note on exponential sums*)

L. CARLITZ in Durham (N. C., U. S. A.)

To Professor L. Rédei on his sixtieth birthday

1. Let p be an odd prime and let ζ denote a primitive p-th root of 1. Put

$$B=\sum_{s=1}^{p-1}c_s\zeta^s \qquad (c_s=\pm 1), \tag{1.1}$$

where the coefficients c_s independently take on the values ± 1. The number of sums B is evidently 2^{p-1}. Also put

$$B_r=\sum_{s=1}^{r}c_s\zeta^{k_s} \qquad (c_s=\pm 1), \tag{1.2}$$

where $r\leqq p-1$ and

$$1\leqq k_1<k_2<\cdots<k_r\leqq p-1.$$

RÉDEI [1, Theorems 6, 7] has proved the following results.

Theorem *A. The sum B satisfies*

$$(1-\zeta)^{\frac{1}{2}(p-1)}\,\Big|\,B \tag{1.3}$$

if and only if

$$B=\pm\sum_{s=1}^{p-1}\left(\frac{s}{p}\right)\zeta^s; \tag{1.4}$$

that is, if and only if B is a Gauss sum. If (1.3) *does not hold, then B is divisible by at most* $(1-\zeta)^{\frac{1}{4}(p-1)}$*; this will occur if and only if* $p=4m+1$ *and*

$$B=\pm(\eta_0-\eta_2)\pm(\eta_1-\eta_3),$$

where g is a primitive root (mod p) *and*

$$\eta_j=\sum_{s=0}^{m-1}\zeta^{g^{4s+j}} \qquad (j=0,1,2,3).$$

*) Research prepared under National Science Foundation grant NSF—G 9425.

Theorem *B*. *If* B_r *satisfies*

$$(1-\zeta)^e \mid B_r, \tag{1.5}$$

then $e \leqq \frac{1}{2}r$.

The proof of these results depend upon some theorems concerning lacunary polynomials in the finite field $GF(p)$.

It may be of interest to note some corollaries of RÉDEI's theorems. If B is defined by (1.1) we may ask when B satisfies

$$|B|^2 = p. \tag{1.6}$$

Since

$$|B|^2 = B\bar{B}, \qquad \bar{B} = \sum_{s=1}^{p-1} c_s \zeta^{-s},$$

it is evident that $|B|^2$ is an integer of the cyclotomic field $R(\zeta)$, where R denotes the rational field. Hence, in place of (1.6), we may ask when B satisfies the weaker condition

$$|B|^2 \equiv 0 \pmod{p}. \tag{1.7}$$

Since $\mathfrak{p} = (1-\zeta)$ is a prime ideal of $R(\zeta)$ such that $(p) = \mathfrak{p}^{p-1}$, (1.7) is equivalent to

$$B\bar{B} \equiv 0 \quad (\mathfrak{p}^{p-1}). \tag{1.8}$$

Now suppose that

$$\mathfrak{p}^e \mid B, \qquad \mathfrak{p}^{e+1} \nmid B; \tag{1.9}$$

applying the automorphism $\zeta \to \zeta^{-1}$, it is clear that (1.9) implies

$$\mathfrak{p}^e \mid \bar{B}, \qquad \mathfrak{p}^{e+1} \nmid \bar{B}.$$

It follows that

$$\mathfrak{p}^{2e} \mid B\bar{B}, \qquad \mathfrak{p}^{2e+1} \nmid B\bar{B}. \tag{1.10}$$

Comparing (1.10) with (1.8), we infer that

$$2e \geqq p-1. \tag{1.11}$$

Thus (1.8) implies (1.3) and therefore by the first of RÉDEI's results quoted above it follows that (1.4) holds. We may accordingly state

Theorem 1. *The sum B satisfies* (1.7) *if and only if* (1.4) *holds, that is if and only if B is a Gauss sum.*

As an immediate corollary, we have

Theorem 2. *The sum B satisfies* (1.6) *if and only is B if a Gauss sum.*

2. If we use the fuller notation

$$B(\zeta^k)=\sum_{s=1}^{p-1} c_s\zeta^{sk} \qquad (1\leqq k\leqq p-1), \tag{2.1}$$

where, as above, $c_s=\pm 1$, then we have

$$\sum_{k=1}^{p-1}|B(\zeta^k)|^2=\sum_{k=1}^{p-1}\sum_{s=1}^{p-1}c_s\zeta^{sk}\sum_{t=1}^{p-1}c_t\zeta^{-tk}=\sum_{s,\,t=1}^{p-1}c_sc_t\sum_{k=1}^{p-1}\zeta^{(s-t)k}.$$

We shall assume that the c_s satisfy the condition

$$\sum_{s=1}^{p-1}c_s=0. \tag{2.2}$$

Then it is clear from the above that

$$\sum_{k=1}^{p-1}|B(\zeta^k)|^2=\sum_{s,\,t=1}^{p-1}c_sc_t\sum_{k=0}^{p-1}\zeta^{(s-t)k}=p\sum_{s=1}^{p-1}c_s^2,$$

so that

$$\sum_{k=1}^{p-1}|B(\zeta^k)|^2=p(p-1). \tag{2.3}$$

According to (2.3), the number $|B(\zeta^k)|^2$ is on the average equal to p. In view of the restriction (2.2), the number of sums $B(\zeta^k)$, for fixed ζ^k, is $\binom{p-1}{m}$, where $p=2m+1$; by Theorem 2, only two of the sums satisfy (1.6). Hence if $B(\zeta^k)$ is not a Gauss sum but (2.2) is satisfied, it follows from (2.3) that both inequalities

$$|B(\zeta^k)|^2>p, \qquad |B(\zeta^k)|^2<p$$

are satisfied for appropriate values of k. This suggests the problem of determining upper and lower bounds for $|B(\zeta^k)|$. However for $\zeta=e^{2\pi i/p}$,

$$c_1=\cdots=c_m=1, \qquad c_{m+1}=\cdots=c_{2m}=-1, \tag{2.4}$$

where $p=2m+1$, we have

$$B=B(\zeta)=\sum_{s=1}^{m}\zeta^s-\sum_{s=m+1}^{2m}\zeta^s=\zeta(1-\zeta^m)\sum_{s=0}^{m-1}\zeta^s=\frac{\zeta(1-\zeta^m)^2}{1-\zeta},$$

so that

$$|B|=\left|\frac{(1-\zeta^m)^2}{1-\zeta}\right|=2\,\frac{\sin^2\dfrac{m\pi}{p}}{\sin\dfrac{\pi}{p}}.$$

Therefore for large p we get

$$|B| \sim \frac{2}{\pi} p.$$

In particular, the statement

(2.6) $$B = o(p)$$

for all B satisfying (2.2), is false.

Again for the choice

(2.7) $$c_1 = c_3 = \cdots = c_{2m-1} = 1, \qquad c_2 = c_4 = \cdots = c_{2m} = -1,$$

we have

$$B = B(\zeta) = \sum_{s=1}^{2m} (-1)^{s-1} \zeta^s = \frac{\zeta(1-\zeta^{2m})}{1+\zeta},$$

so that

$$|B| = \left| \frac{1-\zeta^{2m}}{1+\zeta} \right| = \frac{\sin \frac{2m\pi}{p}}{\cos \frac{\pi}{p}} = \frac{\sin \frac{\pi}{p}}{\cos \frac{\pi}{p}}.$$

For large p this implies

(2.8) $$B \sim \frac{\pi}{p}.$$

Thus the statement

(2.9) $$|B| > c > 0$$

for all B satisfying (2.2) where c is independent of p, is also false. It seems plausible that

(2.10) $$\frac{\pi}{p} < |B| < \frac{2p}{\pi}$$

for all B satisfying (2.2).

3. Turning now to B_r defined by (1.2) we may apply the argument used in the proof of Theorem 1 together with Theorem *A* of RÉDEI to prove the following result.

Theorem 3. *If $r < p-1$, the congruence*

(3.1) $$|B_r|^2 \equiv 0 \pmod{p}$$

holds for no

$$B_r = \sum_{s=1}^{r} c_s \zeta^{k_s} \qquad (c_s = \pm 1),$$

where $1 \leqq k_1 < k_2 < \cdots < k_r < p-1$. A fortiori the equality

(3.2) $$|B_r|^2 = p$$

holds for no B_r.

If we put

$$B_r(\zeta^h) = \sum_{s=1}^{r} c_s \zeta^{k_s h} \qquad (1 \leqq h \leqq p-1), \tag{3.3}$$

and in addition assume that

$$\sum_{s=1}^{r} c_s = 0, \tag{3.4}$$

then exactly as in the proof of (2.3), we have

$$\sum_{h=1}^{p-1} |B_r(\zeta^h)|^2 = pr. \tag{3.5}$$

Thus, when (3.4) is satisfied, $|B_r(\zeta^h)|^2$ is on the average equal to $pr/(p-1)$; for large p, the average is therefore r.

Clearly (3.4) requires that r be even. Put $r=2t$, $\zeta = e^{2\pi i/p}$, $p=2m+1$, and consider

$$B_r = \sum_{s=1}^{t} \zeta^s = \sum_{s=m+1}^{m+t} \zeta^s = \frac{\zeta(1-\zeta^m)(1-\zeta^t)}{1-\zeta}. \tag{3.6}$$

Then

$$|B_r| = \frac{2 \sin \frac{m\pi}{p} \sin \frac{t}{p}}{\sin \frac{\pi}{p}}.$$

For large p it follows that

$$|B_r| \sim \frac{2p}{\pi} \sin \frac{t\pi}{p}. \tag{3.7}$$

In particular if $r = o(p)$, (3.7) yields

$$|B_r| \sim r. \tag{3.8}$$

In the next place, if we take

$$B_r = \sum_{s=1}^{r} (-1)^{s-1} \zeta^s = \frac{\zeta(1-\zeta^r)}{1+\zeta}, \tag{3.9}$$

then

$$|B_r| = \frac{\sin \frac{t\pi}{p}}{\cos \frac{\pi}{p}},$$

so that for large p it follows that

$$|B_r| \sim \sin \frac{t\pi}{p}. \tag{3.10}$$

In particular if $r=o(p)$, (3.10) becomes

$$|B_r| \sim \frac{r\pi}{2p}. \tag{3.11}$$

4. We now give another proof of RÉDEI's theorem that (1.3) holds only when B is a Gauss sum. In the first place (1.3) is equivalent to

$$\sum_{s=1}^{p-1} s^j c_s \equiv 0 \pmod{p} \qquad \left(1 \leqq j < \frac{1}{2}(p-1)\right). \tag{4.1}$$

This is essentially the Lemma on p. 287 of [1]. Indeed, (4.1) follows easily from the identity

$$B = \sum_{s=1}^{p-1} c_s \zeta^s = \sum_{s=1}^{p-1} c_s (1+(\zeta-1))^s = \sum_{j=0}^{p-1} (\zeta-1)^j \sum_{s=j}^{p-1} \binom{s}{j} c_j.$$

Now consider the polynomial $f(x)$ with coefficients in the $GF(p)$ such that

$$f(0)=0, \quad f(s)=c_s \qquad (s=1,\ldots,p-1).$$

Clearly

$$f(x) = -\sum_{s=1}^{p-1} c_s \frac{x^p-x}{x-s} = -\sum_{s=1}^{p-1} c_s (x-s)^{p-1}.$$

It follows from (4.1) that

$$\deg f(x) \leqq m = \frac{1}{2}(p-1). \tag{4.2}$$

Since

$$f^2(0)=0, \quad f^2(s)=1 \qquad (s=1,\ldots,p-1),$$

it follows at once that

$$f^2(x) = x^{p-1}; \tag{4.3}$$

in view of (4.2), it is clear that (4.3) is an identity (and not merely a congruence mod (x^p-x)). Now put

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m \qquad (a_j \in GF(p));$$

making use of (4.3) we get

$$f(x) = \pm x^m = \pm\left(\frac{x}{p}\right).$$

This evidently completes the proof of the theorem.

To prove the second half of Theorem A we require a little more. Suppose that B satisfies

$$\mathfrak{p}^t | B, \qquad \mathfrak{p}^{t+1} \nmid B \tag{4.4}$$

for some t in the range $1 \leqq t \leqq m$. As above we define the polynomial $f(x)$ such that

$$f(0)=0, \quad f(s)=c_s \qquad (s=1,\ldots,p-1).$$

Now (4.4) is equivalent to

$$\sum_{s=1}^{p-1} s^j c_s \begin{cases} \equiv 0 \pmod p & (1 \leqq j < t) \\ \not\equiv 0 \pmod p & (j=t); \end{cases} \tag{4.5}$$

it follows that

$$\deg f(x) = p-1-t. \tag{4.6}$$

Put

$$U(x)=\prod_{c_s=1}(x-s), \qquad V(x)=\prod_{c_s=-1}(x-s),$$

so that

$$x^{2m}-1 = U(x)V(x), \qquad \deg U(x) = \deg V(x) = m. \tag{4.7}$$

Thus $f(x)$ is uniquely determined by

$$\begin{cases} f(x) \equiv 1 \pmod{U(x)}, \\ f(x) \equiv -1 \pmod{V(x)}, \\ f(x) \equiv 0 \pmod{x}. \end{cases} \tag{4.8}$$

It is easily verified that the system (4.8) has the solution

$$f(x) = x(U(x)V'(x)-U'(x)V(x)). \tag{4.9}$$

In the next place, it follows from (4.5) and (4.7) that

$$U(x)=x^m+a_1x^{m-1}+\cdots+a_m, \qquad V(x)=x_m+b_1x^{m-1}+\cdots+b_m, \tag{4.10}$$

where $b_t=-a_t \neq 0$. Substituting in (4.9) we get

$$f(x) = 2ta_tx^{2m-t}+\ldots,$$

so that

$$\deg f(x) = 2m-t. \tag{4.11}$$

Now assume that

$$\frac{1}{2}m < t < m. \tag{4.12}$$

Using (4.7) and (4.10) we get, since $2m-2t<m$,

$$b_j = -a_j \qquad (t \leqq j \leqq m).$$

However, the coefficient of x^{2m-2t} in $U(x)V(x)$ is equal to $-a_t^2 \neq 0$. Thus (4.12) is not possible. Consequently, when $t<m$, we must have $t \leqq \frac{1}{2}m$.

For $t=\frac{1}{2}m$, the coefficient of x^{m-1} in $U(x)V(x)$ is

$$-2a_ta_{t+1}=0,$$

so that $a_{t+1}=0$. Similarly we find that

$$a_j=0 \qquad (t<j<m).$$

Thus (4.7) becomes

$$(x^{2m}-1)=(x^m+a_tx^t+a_m)(x^m-a_tx^t+b_m),$$

where

$$a_m+b_m=a_t^2, \qquad a_mb_m=-1, \qquad a_m=b_m.$$

Put $a_m=\sigma$, where $\sigma^2=-1$, then

$$a_t^2=2\sigma=(\sigma+1)^2,$$

so that $a_t=\sigma+1$. Hence we have

$$A(x)=x^m+(\sigma+1)x^t+\sigma=(x^t+1)(x^t+\sigma),$$
$$B(x)=x^m-(\sigma+1)x^t+\sigma=(x^t-1)(x^t-\sigma).$$

The second half of Theorem *A* now follows immediately.

We have incidentally proved the following result.

Theorem 4. *The sum B satisfies* (4.4) *for some t in the range* $1\leqq t\leqq m$ *if and only if there exists a factorization*

$$x^{2m}-1=(x^m+a_tx^{m-t}+\cdots+a_m)(x^m+b_tx^{m-t}+\cdots+b_t), \tag{4.13}$$

where $a_tb_t\neq 0$.

For $t=m$ or $\frac{1}{2}m$ the possible factorizations (4.13) are described by Theorems 1 and 2 of RÉDEI's paper. It is easy to show that when $t|m$ such factorizations exist. Indeed, if $m=tk$, k odd, we have

$$x^m-1=(x^t-1)(x^{(k-1)t}+x^{(k-2)t}+\cdots+1),$$
$$x^m+1=(x^t+1)(x^{(k-1)t}-x^{(k-2)t}+\cdots+1)$$

and we get the factors

$$U=x^m-2x^{m-t}+\cdots-1, \qquad V=x^m+2x^{m-t}+\cdots+1.$$

For k even, let σ be an integer such that $\sigma^k=-1$; then

$$x^m+1=x^{tk}-\sigma^k=(x^t-\sigma)(x^{(k-1)t}+\sigma x^{(k-2)t}+\cdots+\sigma^{k-1})$$

and we get the factors

$$U=x^m+(\sigma-1)x^{m-t}+\cdots+\sigma^{k-1}, \qquad V=x^m-(\sigma-1)x^{m-t}+\cdots+\sigma.$$

However the condition $t|m$ is not necessary. For example when $p=17$, $t=3$, a possible factor is

$$x^8-x^5+4x^3-8x^2+8x-4=$$
$$(x-1)(x+2)(x+3)(x-4)(x+5)(x-6)(x-7)(x+8).$$

For $p=19$, $t=4$, a factorization (4. 13) is apparently not possible. Assume that

$$x^{18}-1=(x^9-x^5+ax^4+bx^3+cx^2+dx+e)\cdot$$
$$\cdot(x^9+x^5+a'x^4+b'x^3+c'x^2+d'x+e');$$

there is no loss in generalization in normalizing the coefficient of x^5. We find first that

$$a'=-a, \qquad b'=-b, \qquad c'=-c.$$

Also we get the conditions

$$a^2=2b, \qquad ab=c, \qquad -2bc-(e'-e)+a(d'-d)=0,$$
$$-c^2+a(e'-e)+b(d'-d)=0, \qquad b(e'-e)+c(d'-d)=0.$$

Now the last three equations imply

$$\begin{vmatrix} -2bc & -1 & a \\ -c^2 & a & b \\ 0 & b & c \end{vmatrix}=c(2b^3-c^2-3abc)=0.$$

Since $abc\neq 0$, we get, using $ab=c$,

$$b^3=2c^2.$$

But $a^2=2b$, $ab=c$ imply $c^2=2b^3$, so that we have a contradiction.

Thus the question remains open what values of t is the range $1\leqq t<\frac{1}{2}m$ can satisfy (4. 4).

Reference

[1] L. Rédei, Zwei Lückensätze über Polynome in endlichen Primkörpern mit Anwendung auf die endlichen Abelschen Gruppen und die Gaußischen Summen, *Acta Math.*, **79** (1947), 273—290.

(Received September 7, 1959)

Über das nicht ausgeartete Rédeische schiefe Produkt $G \circ \Gamma$

Von Z. JANKO in Lištica (Jugoslavien)

Prof. L. Rédei zum 60. Geburtstag

§ 1. Einleitung

L. RÉDEI hat in der großen Arbeit [3] das schiefe Produkt $G \circ \Gamma$ zweier Gruppen G, Γ mit den Elementen (a, α) $(a \in G, \alpha \in \Gamma)$ und der Produktregel

$$(a, \alpha)(b, \beta) = (a b^{\alpha} \beta^{\alpha}, a^{b} \alpha^{b} \beta) \tag{1}$$

allgemein untersucht, wobei $b^{\alpha}, \beta^{\alpha}; a^{b}, \alpha^{b}$ Funktionen der angegebenen Argumente mit Werten aus G bzw. Γ sind, und die Bedingungen dafür aufgestellt, daß $G \circ \Gamma$ eine Gruppe mit der Einheit (e, ε) ist (wo e bzw. ε das Einselement von G bzw. Γ ist). Diese Bedingungen sind (vgl. RÉDEI [3], § 3):

$$a^{\varepsilon} = a, \quad e^{\alpha} = \varepsilon^{\alpha} = \alpha^{\varepsilon} = e, \quad \alpha^{e} = \alpha, \quad \varepsilon^{\alpha} = e^{\alpha} = a^{e} = \varepsilon, \tag{2}$$

$$c^{a^{b}} = c, \quad \gamma^{\alpha^{\beta}} = \gamma, \tag{3}$$

$$\gamma^{a^{b}} = e, \quad c^{\alpha^{\beta}} = \varepsilon, \tag{4}$$

$$b^{\alpha} c^{\alpha^{b}} = (bc)^{\alpha} (b^{c})^{\alpha}, \quad \gamma^{\alpha^{\beta}} \beta^{\alpha} = (\beta^{\gamma})^{\alpha} (\gamma^{\beta})^{\alpha}, \tag{5}$$

$$\beta^{\alpha} c^{\alpha^{\beta}} = (c^{\beta})^{\alpha} (\beta^{c})^{\alpha}, \quad \gamma^{b^{a}} b^{a} = (b^{\gamma})^{a} (\gamma^{b})^{a}, \tag{6}$$

$$\beta^{\alpha} \gamma^{\alpha^{\beta}} = (\gamma^{\beta})^{\alpha} (\beta\gamma)^{\alpha}, \quad c^{b^{a}} b^{\alpha} = (cb)^{a} (c^{b})^{\alpha}, \tag{7}$$

$$(b^{c}\gamma)^{\alpha} = (b^{c})^{\alpha} \gamma^{\alpha}, \quad (c\beta^{\gamma})^{\alpha} = c^{a} (\beta^{\gamma})^{\alpha}, \tag{8}$$

$$\gamma^{\alpha^{c\beta}\beta^{c}} = \gamma^{\alpha\beta}, \quad c^{b^{\gamma}a^{\gamma^{b}}} = c^{ba}. \tag{9}$$

Wenn diese Bedingungen erfüllt sind, dann sprechen wir über eine (Rédeische) Gruppe $G \circ \Gamma$.

Aus (2) bis (9) folgen noch weitère Gleichungen:

$$\gamma^{\alpha^{c}} = \gamma^{\alpha}, \quad c^{a^{\gamma}} = c^{a}, \tag{10}$$

$$c^{a^{b}\beta} = c^{\beta}, \quad \gamma^{b\,a^{\beta}} = \gamma^{b}. \tag{11}$$

Sind genau k der vier Relationen $b^\alpha = b$, $\beta^\alpha = e$, $a^b = \varepsilon$, $\alpha^b = \alpha$ identisch erfüllt, wo e bzw. ε das Einselement von G bzw. Γ ist, so heißt $G \circ \Gamma$ k-fach ausgeartet. Im Falle $k = 0$ nennen wir $G \circ \Gamma$ nichtausgeartet.

Es gibt nur vier wesentlich verschiedene zweifach ausgeartete Fälle:

$$G^1\Gamma\colon\ (a, \alpha)(b, \beta) = (ab, a^b \alpha^b \beta),$$

$$G^2\Gamma\colon\ (a, \alpha)(b, \beta) = (ab^\alpha, \alpha^b \beta),$$

$$G^3\Gamma\colon\ (a, \alpha)(b, \beta) = (ab\beta^\alpha, a^b \alpha\beta),$$

$$G^4\Gamma\colon\ (a, \alpha)(b, \beta) = (ab^\alpha, a^b \alpha\beta),$$

von denen die ersten zwei gerade die Schreierschen Erweiterungen von Γ mit G bzw. die Zappa—Szépschen Produkte von G und Γ darstellen.

KOCHENDÖRFFER [2] untersuchte die übrigen zwei Spezialfälle und stellte fest, daß die durch $G^3\Gamma$, $G^4\Gamma$ gelieferten Gruppen sich als zweimal hintereinander ausgeführte Schreiersche Erweiterungen erzeugen lassen, wobei jedesmal die bei den Erweiterungen auftretenden Bestimmungsstücke sich aus den Angaben G, Γ und aus den ebenfalls angegebenen Funktionen β^α, a^b bzw. b^α, a^b festlegen lassen.

RÉDEI [4] stellte die Frage, ob mit dem Verfahren aus [2] sich sogar jede Gruppe $G \circ \Gamma$ in einige hintereinanderfolgende Konstruktionen von der Art $G^1\Gamma$, $G^2\Gamma$ zerlegen lasse. F. RÜHS [6] sagt, daß die Beantwortung dieser Frage sehr schwierig sei. Er gibt eine Antwort für den Fall der einfach ausgearteten Gruppen:

$$G*\Gamma\colon\ (a, \alpha)(b, \beta) = (ab\beta^\alpha, a^b \alpha^b \beta)$$

$$G**\Gamma\colon\ (a, \alpha)(b, \beta) = (ab^\alpha, a^b \alpha^b \beta)$$

und zwar stellt er fest, daß $G*\Gamma$ eine zweimalige Schreiersche Erweiterung gewisser Untergruppen, während $G**\Gamma$ eine einfache Schreiersche Erweiterung gewisser Untergruppen ist, von denen die eine ein Zappa—Szépsches Produkt ist.

TIBILETTI [7] untersuchte die nicht ausgeartete Gruppe $G \circ \Gamma$, hat aber nur gezeigt, daß die Gruppe $G \circ \Gamma$ sich mit zwei Schreierschen Erweiterungen und mit einem Produkt zweier vertauschbaren Gruppen herstellen läßt. Da der Durchschnitt dieser vertauschbaren Gruppen nicht immer das Einselement ist, somit dieses Produkt im allgemeinen kein Zappa—Szépsches Produkt zu sein braucht (vgl. [5]), so haben wir im nichtausgearteten Fall noch nicht die vollständige Beantwortung der Rédeischen Frage.

Wir betrachten die (nicht ausgeartete) Rédeische Gruppe $G \circ \Gamma$, bestimmt durch vier Funktionen $b^\alpha, \beta^\alpha, a^b, \alpha^b$. Dann gelten die Bedingungen (2) bis (11).

Hält man in den zwei Funktionen $c^\beta (\in G)$, $\gamma^b (\in \Gamma)$ den Operator β bzw. b fest und läßt das Grundelement varieren, so entstehen zwei Abbildungen, die wir in der Form

$$c \to c^\beta \quad (c \in G), \quad \gamma \to \gamma^b \quad (\gamma \in \Gamma) \tag{12}$$

bezeichnen. In [3] § 4 hat RÉDEI bemerkt, daß zur näheren Untersuchung der Gruppe $G \circ \Gamma$ diese Abbildungen gute Dienste leisten können, aber diese Abbildungen verhalten sich im allgemeinen recht kompliziert.

In JANKO [1] wurde gezeigt, daß die Abbildungen (12) Permutationen von G bzw. Γ sind und wenn wir

$${}^\beta a = \left(\beta^{\beta^{-1}}\right)^{-1} a^{\beta^{-1}} \left(\beta^{\left(\beta^{\beta^{-1}}\right)^{-1} a^{\beta^{-1}}}\right)^{\beta^{-1}}, \tag{13}$$

$${}^b \alpha = \left(b^{\alpha^{b^{-1}} \left(b^{b^{-1}}\right)^{-1}}\right)^{b^{-1}} \alpha^{b^{-1}} \left(b^{b^{-1}}\right)^{-1} \tag{14}$$

setzen, dann gelten die Beziehungen

$$({}^\beta a)^\beta = a, \quad ({}^b \alpha)^b = \alpha. \tag{15}$$

Wie üblich, nennen wir eine Untergruppe $L(\Delta)$ von $G(\Gamma)$ zulässig, wenn sie bei den Permutationen $c \to c^\beta$ $(\gamma \to \gamma^b)$ in sich abgebildet wird. Wegen (13), (14) und (15) gilt: Wenn eine zulässige Untergruppe $L(\Delta)$ von $G(\Gamma)$ alle Elemente von der Gestalt $\alpha^\beta (a^b)$ enthält, dann sind die Abbildungen

$$c \to c^\beta (c \in L) \quad (\gamma \to \gamma^b (\gamma \in \Delta)).$$

Permutationen von $L(\Delta)$. Diese seien induzierte Permutationen genannt.

In dieser Arbeit untersuchen wir weiter die nichtausgeartete Rédeische Gruppe $G \circ \Gamma$ und zeigen insbesondere, daß gewisse nichtausgeartete Gruppen $G \circ \Gamma$ sich sogar mit drei Schreierschen Erweiterungen herstellen lassen.

§ 2. Eigenschaften gewisser Komplexe von G und Γ

RÉDEI [3] definierte die folgenden vier Komplexe:

G_1 besteht aus den a mit $\alpha^a = \alpha \ (= \alpha^1)$,

G_0 „ „ „ a „ $b^a = \varepsilon \ (= \alpha^0)$,

Γ_1 „ „ „ α „ $a^\alpha = a \ (= a^1)$,

Γ_0 „ „ „ α „ $\beta^\alpha = e \ (= a^0)$,

wo e bzw. ε das Einselement von G bzw. Γ ist. Es gilt $e \in G_1, G_0$, $\varepsilon \in \Gamma_1, \Gamma_0$. Ferner lassen sich (3), (4) so aussprechen:

$$a^b \in \Gamma_1, \Gamma_0; \quad \alpha^\beta \in G_1, G_0.$$

RÉDEI bemerkte auch, daß $G \circ \Gamma$ dann und nur dann ausgeartet ist, wenn mindestens eine der Gleichungen

$$G_1 = G, \quad G_0 = G, \quad \Gamma_1 = \Gamma, \quad \Gamma_0 = \Gamma$$

gilt. Wir werden hier einige Eigenschaften dieser Komplexe beweisen.

Satz 1. *Die komplexe G_0, Γ_0 sind zulässige Untergruppen von G bzw. Γ.*

Beweis. Wenn $a_0, b_0 \in G_0$ ist, dann ist $c^{a_0} = \varepsilon$ und $c^{b_0} = \varepsilon$ für alle $c \in G$. Nach (7_2) ist $c^{b_0 a_0} = \varepsilon$. Aus (7_2) folgt ferner für $b = b_0$, $a = b_0^{-1}$

$$b_0^{b_0^{-1}} = (c b_0)^{b_0^{-1}},$$

woraus für $c = b_0^{-1}$ sich

$$b_0^{b_0^{-1}} = \varepsilon$$

ergibt. Also ist

$$(c b_0)^{b_0^{-1}} = \varepsilon.$$

Für $c = a b_0^{-1}$ folgt hieraus endlich

$$a^{b_0^{-1}} = \varepsilon$$

für alle $a \in G$. Der Komplex G_0 ist also eine Untergruppe von G. Diese Untergruppe ist auch zulässig, denn nach (10_2) ist

$$c^{b_0^{\alpha}} = c^{b_0} = \varepsilon.$$

Ähnlich beweist man mit Hilfe von (7_1) und (10_1), daß der Komplex Γ_0 eine zulässige Untergruppe von Γ ist.

Korollar. *Die Abbildungen $c \to c^{\beta}$ bzw. $\gamma \to \gamma^{b}$ induzieren Permutationen von G_0 bzw. Γ_0.*

Satz 2. *Die Komplexe $G' = G_0 \cap G_1$ und $\Gamma' = \Gamma_0 \cap \Gamma_1$ sind zulässige Normalteiler von G_0 bzw. Γ_0.*

Beweis. Wenn $a', b' \in G'$ ist, dann ist $b'a' \in G_0$ und $b'^{-1} \in G_0$. Man muß noch beweisen, daß $b'a' \in G_1$ und $b'^{-1} \in G_1$ ist. Nach (6_2) ist $\gamma^{b'a'} = \gamma$ und $\gamma b'^{b'^{-1}} = \gamma^{b'^{-1}}$. Für $\gamma = \varepsilon$ folgt aus der letzten Relation $b'^{b'^{-1}} = \varepsilon$, ferner gilt $\gamma^{b'^{-1}} = \gamma$. Der Komplex G' ist eine Gruppe. Wenn $b' \in G'$ ist, dann ist $b'^{\alpha} \in G_0$ und nach (5_2) ist auch $\gamma^{b'^{\alpha}} = \gamma$. Die Untergruppe G' ist also zulässig. Wenn $a' \in G'$ und $b_0 \in G_0$ ist, dann ist nach (6_2):

$$\gamma^{b_0 a' b_0^{-1}} = (\gamma^{b_0 a'})^{b_0^{-1}},$$

$$\gamma^{b_0 a'} = \gamma^{b_0},$$

$$(\gamma^{b_0})^{b_0^{-1}} = \gamma.$$

Es gilt also

$$\gamma^{b_0 a' b_0^{-1}} = \gamma$$

somit ist G' normal in G_0. Ähnlich beweist man, daß Γ' zulässiger Normalteiler von Γ_0 ist.

Korollar. *Die Abbildungen $c \to c^\beta$ bzw. $\gamma \to \gamma^b$ induzieren Automorphismen von G' bzw. Γ'.*

Nach (5) ist nämlich $(a'b')^\alpha = a'^\alpha b'^\alpha$, $(\alpha'\beta')^\alpha = \alpha'^\alpha \beta'^\alpha$ $(a', b' \in G', \alpha', \beta' \in \Gamma')$.

Satz 3. *Wenn die Gruppe Γ abelsch ist und identisch $a^b = b^a$ gilt, dann ist der Komplex G_1 eine zulässige Untergruppe von G.* (Ähnliches gilt für Γ_1.)

Beweis. Sei $\alpha^{a_1} = \alpha$ und $\alpha^{b_1} = \alpha$ für alle $\alpha \in \Gamma$. Dann folgt aus (6_2)

$$\alpha^{b_1 a_1} b_1^\alpha = (b_1^\alpha)^{a_1} (\alpha^{b_1})^{a_1},$$

also

$$\alpha^{b_1 a_1} b_1^{a_1} = a_1^{b_1^\alpha} \alpha,$$

und daraus ergibt sich wegen (10_2)

$$\alpha^{b_1 a_1} b_1^{a_1} = a_1^{b_1} \alpha,$$

also endlich

$$\alpha^{b_1 a_1} = \alpha.$$

Ferner folgt aus (6_2)

$$\alpha b_1^{-1} = (b_1^\alpha)^{b_1^{-1}} \alpha^{b_1^{-1}},$$

also

$$\alpha b_1^{-1} = (b_1^{-1})^{b_1} \alpha^{b_1^{-1}},$$

d. h.

$$\alpha^{b_1^{-1}} = \alpha.$$

Der Komplex G_1 ist also eine Gruppe.

Aus (5_2) folgt

$$\alpha^{a_1^\beta} \beta = (\beta^\alpha)^{a_1} \alpha\beta,$$

also

$$\alpha^{a_1^\beta} \beta = a_1^{\beta^\alpha} \alpha\beta,$$

d. h. wegen (4_2)

$$\alpha^{a_1^\beta} = \alpha.$$

Die Gruppe G_1 ist also zulässig. Damit ist Satz 4 bewiesen.

In § 3 werden wir den folgenden Satz anwenden.

Satz 4. *Wenn die Abbildungen $\gamma \to \gamma^b$ $(\gamma \in \Gamma)$ nicht nur Permutationen sondern sogar Automorphismen von Γ sind, dann gelten die Beziehungen*

$$b^{-1}b^\alpha \in G_0, \quad b_0^{-1}b_0^\alpha \in G_1$$

für alle $b \in G$, $b_0 \in G_0$, $\alpha \in \Gamma$.

(Natürlich gilt auch der „duale" Satz für Γ_0, Γ_1.)

Beweis. Aus (7_2) und (10_2) folgt

$$c^{b^{-1}b^\alpha}(b^{-1})^b = (cb^{-1})^b (c^{b^{-1}})^{b^\alpha}. \tag{16}$$

Weiter folgt aus (5_2)

$$\left(c^{b^{-1}}\right)^{b^\alpha} \alpha^b = \left(\alpha^{c^{b^{-1}}}\right)^b \left(c^{b^{-1}}\alpha\right)^b$$

und daraus ergibt sich wegen (4_1), (2_4) und $\left(c^{b^{-1}}\alpha\right)^b = \left(c^{b^{-1}}\right)^b \alpha^b$

$$\left(c^{b^{-1}}\right)^{b^\alpha} = \left(c^{b^{-1}}\right)^b. \tag{17}$$

Aus (16) und (17) folgt

$$c^{b^{-1}b^\alpha}(b^{-1})^b = (cb^{-1})^b (c^{b^{-1}})^b. \tag{18}$$

Wieder nach (7_2) ist

$$(b^{-1})^b = (cb^{-1})^b \left(c^{b^{-1}}\right)^b.$$

Hieraus und aus (18) folgt $c^{b^{-1}b^\alpha} = \varepsilon$ also schließlich

$$b^{-1}b^\alpha \in G_0.$$

Wir haben noch die Beziehung $b_0^{-1}b_0^\alpha \in G_1$ $(b_0 \in G_0, \alpha \in \Gamma)$ zu beweisen. Aus (6_2) folgt

$$\gamma^{b_0^{-1}b_0^\alpha} = \left(\gamma^{b_0^{-1}}\right)^{b_0^\alpha}, \tag{19}$$

denn nach Satz 1 gilt $b_0^\alpha \in G_0$. Andererseits folgt aus (5_2) und (10_1)

$$\left(\gamma^{b_0^{-1}}\right)^{b_0^\alpha} \alpha^{b_0} = \left(\gamma^{b_0^{-1}}\alpha\right)^{b_0},$$

also

$$\left(\gamma^{b_0^{-1}}\right)^{b_0^\alpha} = \left(\gamma^{b_0^{-1}}\right)^{b_0}. \tag{20}$$

Ferner ist nach (6_2)

$$\left(\gamma^{b_0^{-1}}\right)^{b_0} = \gamma. \tag{21}$$

Aus (19), (20) und (21) folgt endlich

$$\gamma^{b_0^{-1} b_0^{\alpha}} = \gamma,$$

d. h.

$$b_0^{-1} b_0^{\alpha} \in G_1.$$

Damit ist Satz 4 bewiesen.

Bemerkung. Es existiert die nicht ausgeartete Rédeische Gruppe $G \circ \Gamma$ mit den folgenden Eigenschaften:

a) die Gruppen G, Γ sind abelsch,

b) es gilt identisch $a^b = b^a$, $\alpha^\beta = \beta^\alpha$,

c) es gilt identisch $(ab)^\gamma = a^\gamma b^\gamma$, $(\alpha\beta)^\varepsilon = \alpha^\varepsilon \beta^\varepsilon$.

Das Rédeische Beispiel der nicht ausgearteten Gruppe $G \circ \Gamma$ aus [3] § 14 hat offenbar (wie man leicht einsieht) die verlangten Eigenschaften.

§ 3. Dekomposition gewisser nichtausgearteter Gruppen $G \circ \Gamma$

Die Komplexe G_0, G' haben die Bedeutung aus § 2.

Satz 5. *Ist die Gruppe $G \circ \Gamma$ so beschaffen, daß die Gruppe G abelsch ist und die Abbildungen $\gamma \to \gamma^\varepsilon (\gamma \in \Gamma)$ nicht nur Permutationen von Γ sondern auch Automorphismen von Γ sind, so ist die Menge (G_0, Γ) der Elemente (a_0, α) $(a_0 \in G_0, \alpha \in \Gamma)$ ein Normalteiler von $G \circ \Gamma$ und es gilt*

$$G \circ \Gamma / (G_0, \Gamma) \approx G/G_0, \tag{22}$$

d. h. die Gruppe $G \circ \Gamma$ ist eine Schreiersche Erweiterung von (G_0, Γ) mit G/G_0, wobei die bei der Erweiterung auftretenden Bestimmungsstücke sich aus den Angaben G, Γ und aus den ebenfalls angegebenen Funktionen $b^\alpha, \beta^\alpha, a^b, \alpha^b$ festlegen lassen.

Beweis. Der Komplex (G_0, Γ) ist eine Gruppe, denn es gilt (mit $a_0, b_0 \in G_0$)

$$(a_0, \alpha)(b_0, \beta) = (a_0 b_0^\alpha \beta^\alpha, \alpha^{b_0} \beta),$$

$$(a_0, \alpha)^{-1} = \left((\alpha^{\alpha^{-1}})^{-1}, \alpha^{-1}\right)(a_0^{-1}, \varepsilon)$$

(s. Rédei [3], § 4) und nach Satz 1 ist $a_0 b_0^\alpha \beta^\alpha, (\alpha^{\alpha^{-1}})^{-1}, a_0^{-1} \in G_0$.

Ferner ist (G_0, Γ) normal in $G \circ \Gamma$, denn aus

$$(a_0, \alpha)(b, \beta) = (b, \beta)(c, \gamma), \quad (a_0 \in G_0),$$

folgt

$$(a_0 b^\alpha \beta^\alpha, a_0^b \alpha^b \beta) = (b c^\beta \gamma^\beta, b^\varepsilon \beta^\varepsilon \gamma),$$

also nach Vergleichen der ersten „Komponenten"

$$c^\beta = b^{-1} b^\alpha a_0 \beta^\alpha (\gamma^\beta)^{-1},$$

woraus nach Satz 4 und Korollar von Satz 1 schließlich $c \in G_0$ folgt.

Man setzt

$$G = \sum_{A \in G/G_0} u_A G_0.$$

Die Abbildung

$$A \to (u_A, \varepsilon)(G_0, \Gamma) \quad (A \in G/G_0)$$

zeigt, daß (22) gilt. Die Gruppe $G \circ \Gamma$ ist also eine Erweiterung von (G_0, Γ) mit G/G_0. Jetzt werden wir noch das Faktorensystem und die Automorphismenmenge dieser Erweiterung berechnen. Es gilt für $a_0, b_0 \in G_0$

$$(u_A, \varepsilon)(a_0, \alpha)(u_B, \varepsilon)(b_0, \beta) = (u_A, \varepsilon)(a_0 u_B^\alpha, a_0^{u_B} \alpha^{u_B})(b_0, \beta) =$$
$$= (u_A, \varepsilon)(u_B^\alpha a_0, a_0^{u_B} \alpha^{u_B})(b_0, \beta) = (u_A, \varepsilon)(u_B^\alpha, \varepsilon)(a_0, a_0^{u_B} \alpha^{u_B})(b_0, \beta) =$$
$$= (u_A, \varepsilon)(u_B, \varepsilon)(u_B^{-1} u_B^\alpha, \varepsilon)(a_0, a_0^{u_B} \alpha^{u_B})(b_0, \beta) =$$
$$= (u_A u_B, u_A^{u_B})(u_B^{-1} u_B^\alpha, \varepsilon)(a_0, a_0^{u_B} \alpha^{u_B})(b_0, \beta) =$$
$$= (u_{AB} u_{AB}^{-1} u_A u_B, u_A^{u_B})(u_B^{-1} u_B^\alpha, \varepsilon)(a_0, a_0^{u_B} \alpha^{u_B})(b_0, \beta) =$$
$$= (u_{AB}, \varepsilon)(u_{AB}^{-1} u_A u_B, u_A^{u_B})(u_B^{-1} u_B^\alpha a_0, a_0^{u_B} \alpha^{u_B})(b_0, \beta).$$

Da $u_{AB}^{-1} u_A u_B \in G_0$ und $u_B^{-1} u_B^\alpha \in G_0$ (Satz 4) ist, so ist

$$(u_{AB}^{-1} u_A u_B, u_A^{u_B})$$

das Faktorensystem und jedem $B \in G/G_0$ ist ein Automorphismus

$$(a_0, \alpha) \to (u_B^{-1} u_B^\alpha a_0, a_0^{u_B} \alpha^{u_B})$$

von (G_0, Γ) zugeordnet.

Satz 6. *Ist die Gruppe $G \circ \Gamma$ so beschaffen, daß die Gruppe G abelsch ist und die Abbildungen $\gamma \to \gamma^c$ $(\gamma \in \Gamma)$ nicht nur Permutationen von Γ sondern auch Automorphismen von Γ sind, so ist die Gruppe (G_0, Γ) eine Schreiersche Erweiterung von G' mit einer Schreierschen Erweiterung von Γ mit G_0/G', wobei jedesmal die bei den Erweiterungen auftretenden Bestimmungsstücke sich aus den Angaben G, Γ und aus den angegebenen Funktionen $b^\alpha, \beta^\alpha, a^b, \alpha^b$ festlegen lassen.*

Beweis. Es gilt

$$(G', \varepsilon) \approx G',$$

denn es ist $(a', \varepsilon)(b', \varepsilon) = (a' b', \varepsilon)$ für $a', b' \in G'$. Die Gruppe (G', ε) ist normal

in (G_0, Γ), denn man sieht leicht, daß für $a' \in G', b_0 \in G_0, \beta \in \Gamma$ die Relation

$$(a', \varepsilon)(b_0, \beta) = (b_0, \beta)({}^{\beta}a', \varepsilon)$$

gilt, da $({}^{\beta}a')^{\beta} = a'$ und nach Korollar von Satz 2 auch ${}^{\beta}a' \in G'$ gilt.

Setzt man

$$G_0 = \sum_{A \in G_0/G'} G' v_A,$$

so gilt auch

$$(G_0, \Gamma) = \sum_{(A, \alpha) \in (G_0/G', \Gamma)} (G', \varepsilon)(v_A, \alpha),$$

worin $(G_0/G', \Gamma)$ die Menge aller Elemente (A, α) $(A \in G_0/G', \alpha \in \Gamma)$ bezeichnet. In der Menge $(G_0/G', \Gamma)$ definieren wir das schiefe Produkt $(G_0/G') \circ \Gamma$ mit

$$(A, \alpha)(B, \beta) = (AB, \alpha^{v_B}\beta).$$

Die Abbildung

$$(G', \varepsilon)(v_A, \alpha) \to (A, \alpha)$$

zeigt, daß

$$(G_0, \Gamma)/(G', \varepsilon) \approx (G_0/G') \circ \Gamma$$

ist, denn es gilt nach Satz 4 $v_A v_B^{\alpha} = v_A v_B a' = a_1' v_{AB}$ mit $a', a_1' \in G'$ und wir haben:

$$(G', \varepsilon)(v_A, \alpha)(G', \varepsilon)(v_B, \beta) = (G', \varepsilon)(v_A, \alpha)(v_B, \beta) =$$

$$= (G', \varepsilon)(v_A v_B^{\alpha} \beta^{\alpha}, \alpha^{v_B}\beta) = (G', \varepsilon)(\beta^{\alpha} v_A v_B^{\alpha}, \alpha^{v_B}\beta) =$$

$$= (G', \varepsilon)(\beta^{\alpha}, \varepsilon)(v_A v_B^{\alpha}, \alpha^{v_B}\beta) = (G', \varepsilon)(v_A v_B^{\alpha}, \alpha^{v_B}\beta) =$$

$$= (G', \varepsilon)(a_1' v_{AB}, \alpha^{v_B}\beta) = (G', \varepsilon)(a_1', \varepsilon)(v_{AB}, \alpha^{v_B}\beta) = (G', \varepsilon)(v_{AB}, \alpha^{v_B}\beta).$$

Das schiefe Produkt $(G_0/G') \circ \Gamma$ ist also eine zerfallende Erweiterung von Γ mit G_0/G', ferner ist (G_0, Γ) eine Erweiterung von G' mit $(G_0/G') \circ \Gamma$. Jetzt werden wir noch das Faktorensystem und die Automorphismenmenge dieser letzten Erweiterung berechnen. Das Faktorensystem $(c', \varepsilon) \in (G', \varepsilon)$ bekommen wir aus der Relation

$$(v_A, \alpha)(v_B, \beta) = (c', \varepsilon)(v_{AB}, \alpha^{v_B}\beta)$$

und daraus folgt $c' = v_{AB}^{-1} v_A v_B^{\alpha} \beta^{\alpha} \in G'$ nach Satz 4. Das Automorphismensystem bekommen wir aus der Relation

$$(v_B, \beta)(a', \varepsilon) = (b', \varepsilon)(v_B, \beta),$$

woraus $b' = a'^{\beta}$ folgt. Jedem $(B, \beta) \in (G_0/G') \circ \Gamma$ ist also der Automorphismus

$$(a', \varepsilon) \to (a'^{\beta}, \varepsilon)$$

von (G', ε) zugeordnet. Damit haben wir Satz 6 bewiesen.

Korollar. *Ist die nicht ausgeartete Rédeische Gruppe $G \circ \Gamma$ so beschaffen, daß die Gruppe G abelsch ist und die Abbildungen $\gamma \to \gamma^e$ ($\gamma \in \Gamma$) nicht nur Permutationen von Γ sondern auch Automorphismen von Γ sind, so läßt sich die Gruppe $G \circ \Gamma$ mit drei (im Fall $G_0 = G'$ mit zwei) Schreierschen Erweiterungen darstellen.*

Natürlich gilt auch „der duale Satz" mit Γ_0, Γ''.

Literaturverzeichnis

[1] Z. Janko, Über das nicht ausgeartete Rédeische schiefe Produkt, *Glasnik mat.-fiz. i astr.*, **14** (1959), 285—290.

[2] R. Kochendörffer, Zur Theorie der Rédeischen schiefen Produkte, *Journal f. d. reine u. angew. Math.*, **192** (1953), 96—101.

[3] L. Rédei, Die Anwendung des schiefen Produktes in der Gruppentheorie, *Journal f. d. reine u. angew. Math.*, **188** (1950), 201—227.

[4] L. Rédei, Besprechung der Arbeit [2] im *Zentralblatt f. Math.*, **51** (1954), 256—257.

[5] L. Rédei—J. Szép, Die Verallgemeinerung der Theorie des Gruppenproduktes von Zappa—Casadio, *Acta Sci. Math.*, **16** (1955), 165—170.

[6] F. Rühs, Über die einfach ausgearteten Rédeischen schiefen Produkte, *Journal f. d. reine u. angew. Math.*, **198** (1957), 81—86. [Vgl. auch Z. Janko, Über das Rédeische schiefe Produkt vom Typ $G \odot \Gamma$, *Acta Sci. Math.*, **21** (1960), 4—6.]

[7] C. M. Tibiletti, Una composizione del prodotto sghembo di Rédei, *Collectanea Math. Milano*, **167** (1958), 1 - 15.

(Eingegangen am 28. September 1959)

Some remarks on set theory. VII

By P. ERDŐS and A. HAJNAL in Budapest

Professor L. Rédei on his 60th birthday

§ 1. Introduction

Let $\mathfrak{F}$ be a family of non empty sets and let $\mathfrak{r}$ be a cardinal number. The family $\mathfrak{F}$ is said to possess property $A(\mathfrak{r})$ if there exists a set X with $\overline{\overline{X}} < \mathfrak{r}$ which contains at least one element of each set of the family $\mathfrak{F}$.

Let $p(\mathfrak{F})$ denote the smallest cardinal number $\mathfrak{p}$, for which $\overline{\overline{F}} \leqq \mathfrak{p}$ for every $F \in \mathfrak{F}$.

Let now $\mathfrak{q}$ be a cardinal number. The family $\mathfrak{F}$ is said to possess property $A(\mathfrak{q}, \mathfrak{r})$ if each subfamily $\mathfrak{F}'$ of $\mathfrak{F}$ possesses property $A(\mathfrak{r})$ provided $\overline{\overline{\mathfrak{F}'}} < \mathfrak{q}$. We investigate the following problem: Suppose that the family $\mathfrak{F}$ possesses property $A(\mathfrak{q}, \mathfrak{r})$. Under what conditions on $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ does the family $\mathfrak{F}$ possess property $A(\mathfrak{r})$?

More generally we introduce the symbol $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \rightarrow \mathfrak{s}$ to indicate the statement that every family $\mathfrak{F}$ (with $p(\mathfrak{F}) = \mathfrak{p}$) which possesses property $A(\mathfrak{q}, \mathfrak{r})$ possesses property $A(\mathfrak{s})$ too. ($[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \nrightarrow \mathfrak{s}$ indicates the negation of this statement.)

In Section 2 we are going to prove some results concerning this symbol which using the generalized continuum hypothesis enable us to give a complete discussion for the case $\mathfrak{p} \geqq \aleph_0$.

The problem for finite sets is posed and discussed in a paper of P. ERDŐS and T. GALLAI, and it is not yet entirely solved.[1]) That is why in what follows $\mathfrak{p}$ is supposed to be infinite.

Theorems in the proof of which the generalized continuum hypothesis will be used are marked with a star (*).

In Section 3 we investigate the question what results we can get by using weaker hypotheses or no hypothesis at all. The results in this Section are not quite complete. In Section 4 we investigate an analogous question to that treated in Section 2.

---

[1]) See a forthcoming paper of P. ERDŐS and T. GALLAI.

§ 2.

First we make some obvious remarks.

(1) $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \dashv\!\rightarrow \mathfrak{s}$ if $\mathfrak{s} < \mathfrak{r}$, for every $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$;

(2) $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \dashv\!\rightarrow \mathfrak{s}$ if $\mathfrak{q} \leqq \mathfrak{r}$, for every $\mathfrak{p}$ and $\mathfrak{s}$.

The symbol has the following monotonity properties:

(3)
$$[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \rightarrow \mathfrak{s} \text{ implies } [\mathfrak{p}', \mathfrak{q}, \mathfrak{r}] \rightarrow \mathfrak{s} \text{ if } \mathfrak{p} \geqq \mathfrak{p}',$$
$$[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \rightarrow \mathfrak{s} \text{ implies } [\mathfrak{p}, \mathfrak{q}', \mathfrak{r}] \rightarrow \mathfrak{s} \text{ if } \mathfrak{q} \leqq \mathfrak{q}',$$
$$[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \rightarrow \mathfrak{s} \text{ implies } [\mathfrak{p}, \mathfrak{q}, \mathfrak{r}'] \rightarrow \mathfrak{s} \text{ if } \mathfrak{r} \geqq \mathfrak{r}'$$
$$[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \rightarrow \mathfrak{s} \text{ implies } [\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \rightarrow \mathfrak{s}' \text{ if } \mathfrak{s} \leqq \mathfrak{s}'.$$

We may omit the proofs and in what follows we shall often use these theorems without references.

First we are going to prove the negative results.

The following Lemma 1 gives a general method for the proof of negative theorems concerning the symbol.

For the sake of brevity we introduce the symbol $[\mathfrak{p}, \mathfrak{r}, \mathfrak{s}]^* \rightarrow \mathfrak{q}$ to indicate the following statement:

For every set S with $\overline{\overline{S}} = \mathfrak{p}$ there exists a set $\mathfrak{S}^*$ for which the following conditions hold:

a) every element X of $\mathfrak{S}^*$ is a subset of S of power less than $\mathfrak{s}$,

b) $\overline{\overline{\mathfrak{S}^*}} < \mathfrak{q}$, and

c) every subset Y of S with $\overline{\overline{Y}} < \mathfrak{r}$ is contained in an element of $\mathfrak{S}^*$.

($[\mathfrak{p}, \mathfrak{r}, \mathfrak{s}]^* \dashv\!\rightarrow \mathfrak{q}$ indicates the negation of this statement).

Lemma 1. *Suppose* $\mathfrak{p} \geqq \mathfrak{s} \geqq \mathfrak{r}$. *Then* $[\mathfrak{p}, \mathfrak{r}, \mathfrak{s}]^* \dashv\!\rightarrow \mathfrak{q}$ *implies* $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \dashv\!\rightarrow \mathfrak{s}$

Proof. Let S be a set of power $\mathfrak{p}$. Let $\mathfrak{F}$ be the family containing the complements of the elements of the set $[S]^{<\mathfrak{s}}$ [2]). It is obvious that $p(\mathfrak{F}) = \mathfrak{p}$ and $\mathfrak{F}$ does not possess property $A(\mathfrak{s})$. We have to show that $\mathfrak{F}$ possesses property $A(\mathfrak{q}, \mathfrak{r})$. Let $\mathfrak{F}'$ be a subfamily of $\mathfrak{F}$, $\overline{\overline{\mathfrak{F}'}} < \mathfrak{q}$. Then by the assumption $[\mathfrak{p}, \mathfrak{r}, \mathfrak{s}]^* \dashv\!\rightarrow \mathfrak{q}$ there exists a subset X of S, $\overline{\overline{X}} < \mathfrak{r}$ which is not contained in the complement of any element of $\mathfrak{F}'$, hence $\mathfrak{F}'$ possesses property $A(\mathfrak{r})$.

Corollary 1. *Suppose* $\mathfrak{p} \geqq \mathfrak{q}$ *and* $\mathfrak{p}$ *is regular. Then* $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \dashv\!\rightarrow \mathfrak{s}$ *for* $\mathfrak{s} \leqq \mathfrak{p}$.

Proof. We may suppose $\mathfrak{q} > \mathfrak{r}$ and $\mathfrak{r} \leqq \mathfrak{s}$. But then obviously $[\mathfrak{p}, \mathfrak{r}, \mathfrak{s}]^* \dashv\!\rightarrow \mathfrak{q}$.

---

[2]) $[X]^{<\mathfrak{q}}$ denotes the set of all subsets of X of power less then $\mathfrak{q}$.

Corollary 2. *Suppose* $\mathfrak{p} \geqq \mathfrak{q}$ *and* $\mathfrak{p}$ *is singular. Then* $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \nrightarrow \mathfrak{s}$ *for* $\mathfrak{s} < \mathfrak{p}$.

Proof. Similar to that of Corollary 1.

Corollary 3. *Suppose* $\mathfrak{p}$ *is singular. Put* $\mathfrak{p} = \aleph_\alpha$ *where* α *is of the second kind* $\mathrm{cf}(\alpha) < \alpha$. *Then* $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \nrightarrow \mathfrak{s}$ *for* $\mathfrak{s} \leqq \mathfrak{p}$ *provided* $\mathfrak{q} \leqq \aleph_{\mathrm{cf}(\alpha)}$.

Proof. We may suppose $\mathfrak{q} > \mathfrak{r}$, $\mathfrak{r} \geqq \mathfrak{s}$. We have $[\mathfrak{p}, \mathfrak{r}, \mathfrak{s}]^* \nrightarrow \mathfrak{q}$ in this case too, since the sum of less than $\aleph_{\mathrm{cf}(\alpha)}$ sets each of which has power less than $\aleph_\alpha$, has power less than $\aleph_\alpha$.

Using the same idea we can prove the following negative

Theorem 1. *Suppose* $\mathfrak{p} = \aleph_\alpha$ *is singular,* $\mathfrak{r} > \aleph_{\mathrm{cf}(\alpha)}$ *and* $\mathfrak{q} \leqq \mathfrak{p}^+$. *Then* $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \nrightarrow \mathfrak{s}$ *for* $\mathfrak{s} \leqq \mathfrak{p}$.

Proof. It is enough to prove $[\mathfrak{p}, \mathfrak{p}^+, \aleph_{\mathrm{cf}(\alpha)+1}] \nrightarrow \mathfrak{p}$. By Lemma 1 it is enough to prove $[\aleph_\alpha, \aleph_{\mathrm{cf}(\alpha)+1}, \aleph_\alpha]^* \nrightarrow \aleph_{\alpha+1}$. Let S be a set, $\overline{\overline{S}} = \aleph_\alpha$ and $\mathcal{S}^*$ a set of subsets of S for which $\overline{\overline{\mathcal{S}^*}} < \aleph_{\alpha+1}$, and the elements of which are subsets of S of power less than $\aleph_\alpha$. We have to construct a set $X_0 \subseteq S$ such that $\overline{\overline{X_0}} \leqq \aleph_{\mathrm{cf}(\alpha)}$ and $X_0 \not\subseteq X$ for any element X of $\mathcal{S}^*$. Let $\{\alpha_\nu\}_{\nu < \omega_{\mathrm{cf}(\alpha)}}$ be a monotone increasing sequence of type $\omega_{\mathrm{cf}(\alpha)}$ of ordinal numbers less than α cofinal with α.

Put $\mathcal{S}^*_\nu = \{X : X \in \mathcal{S}^* \text{ and } \overline{\overline{X}} \leqq \aleph_{\alpha_\nu}\}$. We have

$$\mathcal{S}^* = \bigcup_{\nu < \omega_{\mathrm{cf}(\alpha)}} \mathcal{S}^*_\nu .$$

Since $\overline{\overline{\mathcal{S}^*_\nu}} \leqq \aleph_\alpha$ for every ν, we may split S^*_ν into the sum of subsets $S^*_{\nu,\mu}$ for $\mu < \omega_{\mathrm{cf}(\alpha)}$ in such a way that

$$\mathcal{S}^*_\nu = \bigcup_{\mu < \omega_{\mathrm{cf}(\alpha)}} \mathcal{S}^*_{\nu,\mu} \quad \text{and} \quad \overline{\overline{\mathcal{S}^*_{\nu,\mu}}} \leqq \aleph_{\alpha_\mu}$$

for every $\mu < \omega_{\mathrm{cf}(\alpha)}$.

Put $\mathcal{S}^{**}_\lambda = \bigcup_{\nu \leqq \lambda} \bigcup_{\mu \leqq \lambda} \mathcal{S}^*_{\nu,\mu}$ for every $\lambda < \omega_{\mathrm{cf}(\alpha)}$. It is obvious that

$$\mathcal{S}^* = \bigcup_{\lambda < \omega_{\mathrm{cf}(\alpha)}} \mathcal{S}^{**}_\lambda .$$

Let now $(\mathcal{F})$ denote the set $\bigcup_{X \in \mathcal{F}} X$ for an arbitrary family $\mathcal{F}$ of sets.

We have by the construction that

$$\overline{\overline{(\mathcal{S}^{**}_\lambda)}} \leqq \aleph_{\alpha_\lambda} . \aleph_{\alpha_\lambda} . \aleph_{\mathrm{cf}(\alpha)} < \aleph_\alpha$$

for every $\lambda < \omega_{\mathrm{cf}(\alpha)}$. Therefore we can define by transfinite induction a sequence $\{x_\lambda\}_{\lambda < \omega_{\mathrm{cf}(\alpha)}}$ of type $\omega_{\mathrm{cf}(\alpha)}$ of the elements of S in such a way that $x_\lambda \notin \bigcup_{\lambda' < \lambda} (\mathcal{S}^{**}_{\lambda'})$. Put $X_0 = \{x_\lambda\}_{\lambda < \omega_{\mathrm{cf}(\alpha)}}$. It is obvious that X_0 satisfies our requirements.

To obtain positive results we need the following lemmas. Let $\mathfrak{F}$ be an arbitrary family with $(\mathfrak{F}) = S$.

Let $\mathfrak{F}|S'$ denote the family $\{F \cap S'\}_{F \in \mathfrak{F}}$ for an arbitrary subset S' of S.

Lemma 2. *Let $\mathfrak{F}$ be a family $((\mathfrak{F}) = S, p(\mathfrak{F}) = \mathfrak{p})$ which possesses property $A(\mathfrak{q}, \mathfrak{r})$ for certain $\mathfrak{q}$ and $\mathfrak{r}$, where $\mathfrak{q} > \mathfrak{r}$.*

α) Suppose $\mathfrak{q} \leqq \mathfrak{p}^+$, $\mathfrak{q}$ is regular. Then there exists a subset S' of S such that $\overline{\overline{S'}} \leqq p$ and $\mathfrak{F}|S'$ possesses property $A(\mathfrak{q}, \mathfrak{r})$ too.

β) Suppose $\mathfrak{q} > \mathfrak{p}^+$. Then for every $\mathfrak{t}$ with $\mathfrak{r} \cdot \mathfrak{p} \leqq \mathfrak{t} < \mathfrak{q}$ there exists a subset S' of S such that $\overline{\overline{S'}} \leqq \mathfrak{t}$ and $\mathfrak{F}|S'$ possesses property $A(\mathfrak{t}^+, \mathfrak{r})$.

Proof. We are going to prove α). The proof of β) is quite similar and will be omitted. We have formulated β) only to make clear Problems 1 and 2 which will be formulated in Section 3.

If $\mathfrak{r}$ is singular then the family $\mathfrak{F}$ possesses property $A(\mathfrak{q}, \mathfrak{r}')$ for an $\mathfrak{r}' < \mathfrak{r}$, since if corresponding to every $\mathfrak{r}' < \mathfrak{r}$, there exists a subfamily $\mathfrak{F}_{\mathfrak{r}'}$ of $\mathfrak{F}$ such that $\overline{\overline{\mathfrak{F}_{\mathfrak{r}'}}} = \mathfrak{r}'$ and $\overline{\overline{\mathfrak{F}_{\mathfrak{r}'}}}$ does not possess property $A(\mathfrak{r}')$, then the family $\mathfrak{F}' = \bigcup_{\mathfrak{r}' < \mathfrak{r}} \mathfrak{F}_{\mathfrak{r}'}$ has the power $\mathfrak{r} < \mathfrak{q}$ and does not possess property $A(\mathfrak{r})$.

Thus we may suppose $\mathfrak{r}$ to be regular.

Let φ denote the initial number of $\mathfrak{r}$. We are going to define a sequence S_α of subsets of S and a sequence $\mathfrak{F}_\alpha$ of subfamilies of $\mathfrak{F}$ for every $\alpha < \varphi$ by transfinite induction on α as follows.

Let S_0 be an arbitrary subset of S of power $\leqq \mathfrak{p}$.

Suppose now that $\alpha < \varphi$, and the sets S_β as well as the families F_β are already defined for $\beta < \alpha$. Put $S_\alpha^* = \bigcup_{\beta < \alpha} S_\beta$.

Now we distinguish two cases:

(i) $\mathfrak{F}|S_\alpha^*$ does not possess property $A(\mathfrak{q}, \mathfrak{r})$,

(ii) $\mathfrak{F}|S_\alpha^*$ possesses property $A(\mathfrak{q}, \mathfrak{r})$.

Let $\mathfrak{F}_\alpha$ be a subfamily of $\mathfrak{F}$ of power less than $\mathfrak{q}$ such that $\mathfrak{F}_\alpha|S_\alpha^*$ does not possess property $A(\mathfrak{r})$, if (i) holds and put $\mathfrak{F}_\alpha = 0$ if (ii) holds. Put further $S_\alpha = (\mathfrak{F}_\alpha)$. Thus the sets $S_\alpha (0 \leqq \alpha < \varphi)$ and the families F_α $(1 \leqq \alpha < \varphi)$ are defined. Put

$$S_\varphi = \bigcup_{\alpha < \varphi} S_\alpha^* \quad \text{and} \quad \mathfrak{F}_\varphi = \bigcup_{\alpha < \varphi} \mathfrak{F}_\alpha .$$

Now we have $\overline{\overline{S_\alpha}} \leqq \mathfrak{p}$ for every $\alpha < \varphi$ since $p(\mathfrak{F}) = \mathfrak{p}$ and $\overline{\overline{\mathfrak{F}_\alpha}} < \mathfrak{q}$ for every α, hence $\overline{\overline{\mathfrak{F}_\alpha}} \leqq p$ by the assumption $\mathfrak{q} \leqq \mathfrak{p}^+$.

Taking into consideration that $\mathfrak{p}^+ \geqq \mathfrak{q} > \mathfrak{r}$ implies $\mathfrak{r} \leqq \mathfrak{p}$, it follows that $\overline{\overline{S_\alpha^*}} \leqq \mathfrak{p} \cdot \mathfrak{r} = \mathfrak{p}$.

Thus if for an $\alpha < \varphi$ (ii) holds then Lemma 2 is proved.

We have to show that the assumption: for every $\alpha<\varphi$ (i) holds leads to a contradiction. In fact we have $\overline{\overline{\mathcal{F}_\varphi}}<\mathfrak{q}$, since $\overline{\varphi}=\mathfrak{r}<\mathfrak{q}$ and $\mathfrak{q}$ is supposed to be regular. Thus by our assumption it follows that $\mathcal{F}_\varphi$ possesses property $A(\mathfrak{r})$.

It is obvious that $(\mathcal{F}_\varphi)=S_\varphi$. Therefore there exists a set X_0, $X_0\subseteq S_\varphi$ such that $\overline{X_0}<\mathfrak{r}$ and X_0 intersects every element of $\mathcal{F}_\varphi$. But since $\overline{\varphi}=\mathfrak{r}$ is regular there exists an $\alpha_0<\varphi$ such that $X_0\subseteq S^*_{\alpha_0}$. Therefore $\mathcal{F}_\varphi|S^*_{\alpha_0}$ possesses property $A(\mathfrak{r})$, and $\mathcal{F}_{\alpha_0}\subseteq\mathcal{F}_\varphi$ implies that $\mathcal{F}_{\alpha_0}|S^*_{\alpha_0}$ possesses property $A(\mathfrak{r})$ in contradiction with the construction of $\mathcal{F}_{\alpha_0}$.

Lemma 3. *Let $\mathcal{F}$ be a family which possesses property $A(\mathfrak{q},\mathfrak{r})$. Suppose $(\overline{\overline{\mathcal{F}}})=\mathfrak{t}$. The family $\mathcal{F}$ possesses property $A(\mathfrak{s})$, provided* $[\mathfrak{t},\mathfrak{r},\mathfrak{s}]^*\to\mathfrak{q}$.

Proof. Let $\mathcal{S}^*$ be a set of subsets of S satisfying conditions a), b), c) (with $\mathfrak{p}=\mathfrak{t}$). Then one of the elements of $\mathcal{S}^*$ has to intersect every element of $\mathcal{F}$, for if not, we can single out corresponding to every element X of $\mathcal{S}^*$ an element $f(X)$ of $\mathcal{F}$ in such a way that $f(X)\cap X=0$.

Put $\mathcal{F}'=\{f(X)\}_{X\in\mathcal{S}^*}$. Then $\overline{\overline{\mathcal{F}'}}=\overline{\overline{\mathcal{S}^*}}<\mathfrak{q}$ by b) and therefore it possesses property $A(\mathfrak{r})$ in contradiction with c).

Theorem 2. *Suppose $\mathfrak{p}=\aleph_\alpha$ is singular, $\mathfrak{q}>\aleph_{\mathrm{cf}(\alpha)}$, $\mathfrak{r}\leqq\aleph_{\mathrm{cf}(\alpha)}$. Then* $[\mathfrak{p},\mathfrak{q},\mathfrak{r}]\to\mathfrak{p}$.

Proof. It is enough to prove $[\aleph_\alpha,\aleph_{\mathrm{cf}(\alpha)+1},\aleph_{\mathrm{cf}(\alpha)}]\to\aleph_\alpha$. Let $\mathcal{F}$ be a family (with $p(\mathcal{F})=\aleph_\alpha$) which possesses property $A(\aleph_{\mathrm{cf}(\alpha)+1},\aleph_{\mathrm{cf}(\alpha)})$. Since the conditions of Lemma 2 hold, we may suppose that $(\overline{\overline{\mathcal{F}}})=\overline{\overline{S}}=\aleph_\alpha$. Therefore by Lemma 3 it is enough to see that

$$[\aleph_\alpha,\aleph_{\mathrm{cf}(\alpha)},\aleph_\alpha]^*\to\aleph_{\mathrm{cf}(\alpha)+1}.$$

This may be seen as follows: Let $\{x_\varrho\}_{\varrho<\omega_\alpha}$ be a well ordering of S, and let $\{\alpha_\nu\}_{\nu<\omega_{\mathrm{cf}(\alpha)}}$ be a sequence of type $\omega_{\mathrm{cf}(\alpha)}$ of ordinal numbers less than α cofinal with α.

Put $S_\nu=\{x_\varrho:\varrho<\omega_{\alpha_\nu}\}$ and $\mathcal{S}^*=\{S_\nu\}_{\nu<\omega_{\mathrm{cf}(\alpha)}}$. It is well known that

a) $S_\nu\subseteq S$, $\overline{\overline{S_\nu}}<\aleph_\alpha$ for every $\nu<\omega_{\mathrm{cf}(\alpha)}$,

b) $\overline{\overline{\mathcal{S}^*}}=\aleph_{\mathrm{cf}(\alpha)}<\aleph_{\mathrm{cf}(\alpha)+1}$,

c) if $Y\subseteq S$, $\overline{Y}<\aleph_{\mathrm{cf}(\alpha)}$ then Y can not be cofinal with S, and therefore it is contained in one element of $\mathcal{S}^*$.

Corollary 4. *If $\mathfrak{q}>\mathfrak{r}$, then* $[\mathfrak{p},\mathfrak{q},\mathfrak{r}]\to\mathfrak{p}^+$.

Proof. It is enough to show that $[\mathfrak{p},\mathfrak{r}^+,\mathfrak{r}]\to\mathfrak{p}^+$. Using Lemma 2 and 3 we have to show that $[\mathfrak{p},\mathfrak{r},\mathfrak{p}^+]^*\to\mathfrak{r}^+$. But we have trivially $[\mathfrak{p},\mathfrak{r},\mathfrak{p}^+]^*\to 2$.

Corollaries 1—4 and Theorems 1, 2 give a complete discussion of the symbol $[\mathfrak{p},\mathfrak{q},\mathfrak{r}]\to\mathfrak{s}$, for the cases $\mathfrak{p}\geqq\mathfrak{q}$.

In what follows we may suppose $\mathfrak{p} < \mathfrak{q}$ and $\mathfrak{q} > \mathfrak{r}$. Theorem 1 shows that these assumptions do not assure $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \to \mathfrak{r}$. Using the hypothesis we are going to prove that the only exception is that given by Theorem 1. First we prove a theorem which without using the hypothesis can not be proved to be best possible, but using the hypothesis we can obtain from it all results.

Theorem 3. *Suppose* $\mathfrak{q} > \mathfrak{r}$ *with* $\sum_{\mathfrak{r}' < \mathfrak{r}} \mathfrak{p}^{\mathfrak{r}'} < \mathfrak{q}$, *then* $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \to \mathfrak{r}$.

Proof. Put $\mathfrak{t} = \sum_{\mathfrak{r}' < \mathfrak{r}} \mathfrak{p}^{\mathfrak{r}'}$. Then we have

$$\sum_{\mathfrak{r}' < \mathfrak{r}} \mathfrak{t}^{\mathfrak{r}'} = \mathfrak{t} < \mathfrak{t}^{+} \tag{1}$$

and it is enough to prove that $[\mathfrak{t}, \mathfrak{t}^{+}, \mathfrak{r}] \to \mathfrak{r}$.

Let $\mathfrak{F}$ be a family with $p(\mathfrak{F}) = \mathfrak{t}$ which possesses property $A(\mathfrak{t}, \mathfrak{r})$.

Then by Lemma 2 we may suppose $(\overline{\overline{\mathfrak{F}}}) = \mathfrak{t}$ and by Lemma 3 we have to prove only $[\mathfrak{t}, \mathfrak{r}, \mathfrak{r}]^{*} \to \mathfrak{t}^{+}$.

Put $\mathfrak{S}^{*} = [S]^{\mathfrak{r}}$ then S^{*} clearly satisfies conditions a), c) and by (1) it satisfies condition b) too.

(*) Theorem 4. *Suppose* $\mathfrak{p} < \mathfrak{q}$ *with* $\mathfrak{q} > \mathfrak{r}$, *then*

$$[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \to \mathfrak{r}$$

except if $\mathfrak{p} = \aleph_{\alpha}$ *is singular,* $\mathfrak{q} = \aleph_{\alpha+1}$ *and* $\mathfrak{r} > \aleph_{\mathrm{cf}(\alpha)}$.

Proof. We have $\sum_{\mathfrak{r}' < \mathfrak{r}} \mathfrak{p}^{\mathfrak{r}'} \leqq \mathfrak{p}\mathfrak{r} < \mathfrak{q}$ if $\mathfrak{p}$ is regular, or if $\mathfrak{p}$ is singular, but $\mathfrak{r} \leqq \aleph_{\mathrm{cf}(\alpha)}$, and we have $\sum_{\mathfrak{r}' < \mathfrak{r}} \mathfrak{p}^{\mathfrak{r}'} < \mathfrak{p}^{+}\mathfrak{r} < \mathfrak{q}$ if $\mathfrak{q} > \mathfrak{p}^{+}$. The statement of Theorem 4 follows then from Theorem 3 in both cases.

Theorem 4 with Theorem 1 completes the discussion of the symbol $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \to \mathfrak{s}$ for the case $\mathfrak{p} < \mathfrak{r}, \mathfrak{q} > \mathfrak{r}$.

§ 3.

Lemma 4. $[\aleph_{\alpha+n}, \aleph_{\alpha+1}, \aleph_{\alpha+1}]^{*} \to \aleph_{\alpha+n+1}$ *where* n *is finite and* α *is arbitrary.*

The proof of Lemma 4 is a slight modification of the proof of BERNSTEIN's well known equality

$$\aleph_{\alpha+n}^{\aleph_{\alpha}} = \aleph_{\alpha+n}\, \aleph_{\alpha}^{\aleph_{\alpha}}.$$ [3])

[3]) See e. g. A. TARSKI, Quelques théorèmes sur les alephs, *Fundamenta Math*, 7 (1925), 1—14.

Thus we may omit the proof. In the same way one can prove the more general statement

$$[\aleph_{\alpha+n}, \aleph_\alpha, \aleph_\alpha]^* \to \aleph_{\alpha+n+1}$$

if n is finite and $\aleph_\alpha$ is regular.

As a corollary of Lemmas 3, 4 and 5 we obtain the following theorem.

Theorem 5. $[\aleph_{\alpha+n}, \aleph_{\alpha+n+1}, \aleph_\alpha] \to \aleph_\alpha$ *if* $\aleph_\alpha$ *is regular.*

It results that we can obtain all the results concerning the symbol $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \to \mathfrak{s}$ without the hypothesys (*) prowided $\mathfrak{p} < \aleph_\omega$.

We have $[\aleph_\omega, \aleph_{\omega+1}, \aleph_1] \nrightarrow \aleph_\omega$ by Theorem 1 and

$$[\aleph_\omega, \aleph_1, \aleph_0] \begin{matrix} \to \aleph_\omega \\ \nrightarrow \aleph_n \end{matrix}$$

by Theorem 2 and by Corollary 2 respectively. Thus the symbol is completely discussed without the hypotheses for $\mathfrak{p} = \aleph_\omega$.

$\mathfrak{p} = \aleph_{\omega+1}$ is the first cardinal number for which there remains unsolved problem if we do not assume the hypothesis. We can not prove $[\aleph_{\omega+1}, \aleph_{\omega+2}, \aleph_1] \to \aleph_1$ or at least $[\aleph_{\omega+1}, \aleph_{\omega+2}, \aleph_1] \to \aleph_\omega$. ($[\aleph_{\omega+1}, \aleph_{\omega+2}, \aleph_1] \to \aleph_{\omega+1}$ follows from Theorem 5 and $[\mathfrak{p}, \mathfrak{p}^+, \aleph_0] \to \aleph_0$ follows from Theorem 3, since $\sum_{\mathfrak{r}' < \aleph_0} \mathfrak{p}^{\mathfrak{r}'} = \mathfrak{p}$ for every cardinal number $\mathfrak{p}$.)

Lemma 1 shows that a proof of $[\aleph_{\omega+1}, \aleph_{\omega+2}, \aleph_1] \to \aleph_\omega$ proves $[\aleph_{\omega+1}, \aleph_1, \aleph_\omega]^* \to \aleph_{\omega+2}$, i. e. such a proof would furnish a proof of the inequality

$$\aleph_{\omega+1}^{\aleph_0} \leqq \aleph_{\omega+1} \cdot \left(\sum_{n=1}^{\infty} \aleph_n^{\aleph_0} \right) = 2^{\aleph_0} \cdot \aleph_{\omega+1}.$$

It is well known that this is one of the hopeless unsolved problems of set theory.

But we can not decide the truth of the above statement even if we assume this inequality.

Problem 1. Is it true that $\aleph_{\omega+1}^{\aleph_0} \leqq 2^{\aleph_0} \cdot \aleph_{\omega+1}$ implies $[\aleph_{\omega+1}, \aleph_{\omega+2}, \aleph_1] \to \aleph_\omega$?

Lemma 1 shows that $[\mathfrak{p}, \mathfrak{r}, \mathfrak{s}]^* \to \mathfrak{q}$ is a necessary condition of $[\mathfrak{p}, \mathfrak{q}, \mathfrak{r}] \to \mathfrak{s}$ at least in the case $\mathfrak{p} \geqq \mathfrak{s} \geqq \mathfrak{r}$. The problem whether this condition is sufficient or not remains open if we do not assume the generalized continuum hypothesis. Lemma 2 shows only that the condition is sufficient for $\mathfrak{q} \leqq \mathfrak{p}^+$.

Thus it is not quite obvious that $[\aleph_{\omega+1}, \aleph_1, \aleph_1]^* \to \aleph_{\omega+3}$ implies $[\aleph_{\omega+1}, \aleph_{\omega+3}, \aleph_1] \to \aleph_1$.

The part β) of Lemma 2 shows only that $[\aleph_{\omega+2}, \aleph_1, \aleph_1]^* \to \aleph_{\omega+3}$ implies $[\aleph_{\omega+1}, \aleph_{\omega+3}, \aleph_1] \to \aleph_1$. But using the same idea as one uses for the proof of Lemma 4 it is easy to see that the following theorem is valid:

$[\aleph_{\omega+1}, \aleph_1, \aleph_1]^* \to \aleph_{\omega+n+1}$ implies that $[\aleph_{\omega+n}, \aleph_1, \aleph_1]^* \to \aleph_{\omega+n+1}$ and therefore $[\aleph_{\omega+1}\aleph_1, \aleph_1]^* \to \aleph_{\omega+n+1}$ assures the validity of

$$[\aleph_{\omega+1}, \aleph_{\omega+n+1}, \aleph_1] \to \aleph_1.$$

Moreover it is easy to see that $[\aleph_{\omega+1}, \aleph_1, \aleph_1]^* \to \aleph_{\omega+\omega+1}$ implies that $[\aleph_{\omega+1}, \aleph_1, \aleph_1]^* \to \aleph_{\omega+n+1}$ for a finite n and therefore $[\aleph_{\omega+1}, \aleph_1, \aleph_1]^* \to \aleph_{\omega+\omega+1}$ is a sufficient condition for the validity of $[\aleph_{\omega+1}, \aleph_{\omega+\omega+1}, \aleph_1] \to \aleph_1$ too.

The simplest unsolved problem here is

Problem 2. Is the condition $[\aleph_{\omega+1}, \aleph_1, \aleph_1]^* \to \aleph_{\omega+\omega+2}$ sufficient for $[\aleph_{\omega+1}, \aleph_{\omega+\omega+2}, \aleph_1] \to \aleph_1$?

§ 4.

Let $\mathfrak{F}$ be a family of non empty sets and t a cardinal number. The family $\mathfrak{F}$ is said to possess property $B(\mathrm{t})$ if, for every $\mathfrak{F}' \subseteq \mathfrak{F}$ with $\overline{\overline{\mathfrak{F}'}} = \mathrm{t}$, $\mathfrak{F}'$ has a subfamily $\mathfrak{F}''$ with $\overline{\overline{\mathfrak{F}''}} = t$ such that the set $\bigcap_{F \in \mathfrak{F}''} \mathfrak{F}$ is not empty.

We are going to prove the following

Theorem 6. *If the family $\mathfrak{F}$ with $p(\mathfrak{F}) = \mathfrak{p}$ possesses property $B(\mathfrak{p})$, it possesses property $A(\mathfrak{p})$ too.*

Proof. If a family F possesses property $B(\mathfrak{p})$ then the same holds for every subfamily of it. It is easy to see that our theorem holds if $\overline{\overline{\mathfrak{F}}} \leqq \mathfrak{p}$. It follows that a family $\mathfrak{F}$ satisfying the requirements of Theorem 6 possesses property $A(\mathfrak{p}^+, \mathfrak{p})$ hence it has the property $A(\mathfrak{p})$ by Theorem 5, provided $\mathfrak{p}$ is regular.

Therefore we may suppose that $\mathfrak{p}$ is singular $\mathfrak{p} = \aleph_\alpha$ where α is of the second kind, and $\mathrm{cf}(\alpha) < \alpha$. Let $\{\alpha_\nu\}_{\nu < \omega_{\mathrm{cf}(\alpha)}}$ be a sequence of type $\omega_{\mathrm{cf}(\alpha)}$ of ordinal numbers less than α cofinal with α. Put $S = (\mathfrak{F})$. We may suppose $\overline{\overline{S}} \geqq \aleph_\alpha$.

Now we define a double sequence $\{S_{\nu,\mu}\}_{\nu < \omega_{\mathrm{cf}(\alpha)}, \mu < \omega_{\mathrm{cf}(\alpha)}}$ of subsets of S and a sequence $\{\mathfrak{F}_\nu\}_{1 \leqq \nu < \omega_{\mathrm{cf}(\alpha)}}$ of subfamilies of $\mathfrak{F}$, by transfinite induction on ν as follows:

Let S_0 be an arbitrary subset of S of power $\aleph_\alpha$. Let $S_0 = \{x_\varrho^0\}_{\varrho < \omega_\alpha}$ be a well ordering of type ω_α of the set S_0 and put $S_{0,\mu} = \{x_\varrho^0 : \varrho < \omega_{\alpha_\mu}\}$ for every $\mu < \omega_{\mathrm{cf}(\alpha)}$.

It is obvious that

(0) $S_0 = \bigcup_{\mu < \omega_{\mathrm{cf}(\alpha)}} S_{0,\mu}$ and $\overline{\overline{S}}_{0,\mu} \leqq \aleph_{\alpha_\mu}$ for every $\mu < \omega_{\mathrm{cf}(\alpha)}$.

Suppose that the sets $S_{\nu'}$, $S_{\nu',\mu}$ are already defined for every $\nu'<\nu<\omega_{\mathrm{cf}(\alpha)}$ and for every $\mu<\omega_{\mathrm{cf}(\alpha)}$ in such a way that

(00) $\overline{\overline{S}}_{\nu'}=\aleph_\alpha$, $S_{\nu'}=\bigcup_{\mu<\omega_{\mathrm{cf}(\alpha)}} S_{\nu',\mu}$ for every $\nu'<\nu$, and $\overline{\overline{S}}_{\nu'\mu}\leqq\aleph_{\alpha_\mu}$ for every $\nu'<\nu$ and $\mu<\omega_{\mathrm{cf}(\alpha)}$.

Put

$$S_\nu^*=\bigcup_{\nu'<\nu}\bigcup_{\mu<\nu} S_{\nu',\mu}.$$

Then we have by (0) and (00) $\overline{\overline{S}}_\nu^*\leqq\aleph_{\alpha_\nu}\cdot\aleph_{\mathrm{cf}(\alpha)}<\aleph_\alpha$.

If there exists only less than $\aleph_{\alpha_\nu}$ elements of $\mathfrak{F}$ disjoint to S_ν^* then $\mathfrak{F}$ possesses property $A(\aleph_\alpha)$, hence we may assume:

(000) there is an $\mathfrak{F}'\subseteq\mathfrak{F}$ with $\overline{\overline{\mathfrak{F}'}}=\aleph_{\alpha_\nu}$ such that $(\mathfrak{F}')\cap S_\nu^*=0$.

Let $\mathfrak{F}_\nu$ be such a subfamily of $\mathfrak{F}$ and put

$$S_\nu=(\mathfrak{F}_\nu).$$

We have $\overline{\overline{S}}_\nu\leqq\aleph_\alpha$ and we may suppose $\overline{\overline{S}}_\nu=\aleph_\alpha$. Put $S_\nu=\{x_\varrho^\nu\}_{\varrho<\omega_{\mathrm{cf}(\alpha)}}$ and $S_{\nu,\mu}=\{x_\varrho^\nu:\varrho<\omega_{\alpha_\mu}\}$ for every $\mu<\omega_{\mathrm{cf}(\alpha)}$. We have:

(0000) $S_\nu=\bigcup_{\mu<\omega_{\mathrm{cf}(\alpha)}} S_{\nu,\mu}$ and $\overline{\overline{S}}_{\nu,\mu}\leqq\aleph_{\alpha_\mu}$ for every $\mu<\omega_{\mathrm{cf}(\alpha)}$.

Thus S_ν, $S_{\nu,\mu}$ and $\mathfrak{F}_\nu$ are defined and it is proved that (0000) holds for every ν and $\overline{\overline{\mathfrak{F}}}_\nu=\aleph_{\alpha_\nu}$.

Put $S_{\omega_{\mathrm{cf}(\alpha)}}=\bigcup_{\nu<\omega_{\mathrm{cf}(\alpha)}} S_\nu$ and $\mathfrak{F}_{\omega_{\mathrm{cf}(\alpha)}}=\bigcup_{\nu<\omega_{\mathrm{cf}(\alpha)}}\mathfrak{F}_\nu$. We have

$$S_{\omega_{\mathrm{cf}(\alpha)}}=\bigcup_{\nu<\omega_{\mathrm{cf}(\alpha)}}\bigcup_{\mu<\omega_{\mathrm{cf}(\alpha)}} S_{\nu,\mu}=\bigcup_{\mu<\omega_{\mathrm{cf}(\alpha)}}\Big(\bigcup_{\nu'<\nu}\bigcup_{\mu<\nu} S_{\nu'\mu}\Big)=\bigcup_{\nu<\omega_{\mathrm{cf}(\alpha)}} S_\nu^*$$

and therefore

$$(\mathfrak{F}_{\omega_{\mathrm{cf}(\alpha)}})=S_{\omega_{\mathrm{cf}(\alpha)}}=\bigcup_{\nu<\omega_{\mathrm{cf}(\alpha)}} S_\nu^*.$$

On the other hand we have

$$\overline{\overline{\mathfrak{F}}}_{\omega_{\mathrm{cf}(\alpha)}}=\aleph_\alpha.$$

It follows by the assumption that there exists an $\mathfrak{F}'\subseteq\mathfrak{F}_{\omega_{\mathrm{cf}(\alpha)}}$, $\overline{\overline{\mathfrak{F}'}}=\aleph_\alpha$ such that the set $P=\bigcap_{F\in\mathfrak{F}'} F$ is non-empty.

Suppose $x_0\in P$, then $x_0\in(\mathfrak{F}_{\omega_{\mathrm{cf}(\alpha)}})$, hence $x_0\in S_{\nu_0}^*$ for a $\nu_0<\omega_{\mathrm{cf}(\alpha)}$. $\mathfrak{F}'=\bigcup_{\nu<\omega_{\mathrm{cf}(\alpha)}}\mathfrak{F}'\cap\mathfrak{F}_\nu$ since $\mathfrak{F}'\subseteq\mathfrak{F}_{\omega_{\mathrm{cf}(\alpha)}}$ and $\overline{\overline{\mathfrak{F}'}}$ being $\aleph_\alpha$ there exists a $\nu_1\geqq\nu_0$ such that $\mathfrak{F}'\cap\mathfrak{F}_{\nu_1}\neq 0$.

But $S_{\nu_0}^*\subseteq S_{\nu_1}^*$ and therefore $x_0\in(\mathfrak{F}_{\nu_1})\cap S_{\nu_1}^*$ in contradiction with the construction of $\mathfrak{F}_{\nu_1}$ based upon the indirect hypothesis (000).

It follows that the family $\mathcal{F}$ possesses property $A(\aleph_\alpha)$, q. e. d.

Theorem 7. *Suppose* $\mathfrak{p} = \aleph_\alpha$ *is singular and the family* F *(with* $p(\mathcal{F}) = \aleph_\alpha$*) possesses property* $B(\aleph_{\mathrm{cf}(\alpha)})$*, then it possesses property* $A(\aleph_\alpha)$ *too.*

The proof is an easy modification of the proof of Theorem 6 taking for $\mathcal{F}_\nu$ a subfamily of $\mathcal{F}'$ of power 1. We may omit the details.

Remarks. 1. The property $B(\mathfrak{t})$ is not "monotonic" in any direction. The fact that $\mathcal{F}$ possesses property $B(\mathfrak{t})$ implies the same neither for $\mathfrak{t}' < \mathfrak{t}$ nor for $\mathfrak{t}' > \mathfrak{t}$.

2. It is easy to see that a family $\mathcal{F}$ with $p(\mathcal{F}) = \aleph_\alpha$ may possess property $B(\mathfrak{t})$ for every $\mathfrak{t} \leqq \aleph_\alpha$ different from $\aleph_\alpha$ and $\aleph_{\mathrm{cf}(\alpha)}$ without possessing property $A(\aleph_\alpha)$ as shows the example of the family $\mathcal{F}$ which consists of the complements of the elements of $[S]^{<\aleph_\alpha}$ where S is a set of power $\aleph_\alpha$.

3. A family $\mathcal{F}$ with $p(\mathcal{F}) = \aleph_\alpha$ may possess property $B(\mathfrak{t})$ for every $\mathfrak{t} \leqq \aleph_\alpha$ without possessing property $A(\mathfrak{r})$ for any fixed $\mathfrak{r} < \aleph_\alpha$.

In fact let S be a set of power $\aleph_\alpha$. Let $\mathcal{F}$ be the family of the complements of the elements of $[S]^{<\mathfrak{r}}$.

It is obvious that $\mathcal{F}$ possesses property $B(\mathfrak{t})$ for every $\mathfrak{t} < \aleph_\alpha$ and it does not possess property $A(\mathfrak{r})$.

The fact that it possesses property $B(\aleph_\alpha)$ is a corollary of a theorem of P. Erdős.[4])

(Received October 27, 1959)

[4]) See P. Erdős, Some remarks on set theory. III, *Michigan Math. Journal*, **2** (1953), 55.

On a theorem of L. Fejér concerning trigonometric interpolation

By PAUL SZÁSZ in Budapest

To my friend Professor L. Rédei on the occasion of his sixtieth birthday

It is well known that for any trigonometric polynomial

$$\varphi(\vartheta)=a_0+a_1\cos\vartheta+b_1\sin\vartheta+\cdots+a_n\cos n\vartheta+b_n\sin n\vartheta$$

of order $\leqq n$ the values

$$\varphi(\vartheta_0^*)=y_0,\ \varphi(\vartheta_1^*)=y_1,\ \ldots,\ \varphi(\vartheta_n^*)=y_n$$

of $\varphi(\vartheta)$ at the points

$$\vartheta_0^*=\tau,\ \vartheta_1^*=\tau+\frac{2\pi}{n+1},\ \ldots,\ \vartheta_n^*=\tau+n\frac{2\pi}{n+1}$$

determine the value of the integral $\int_0^{2\pi}\varphi(\vartheta)d\vartheta$ uniquely, namely we have

$$\int_0^{2\pi}\varphi(\vartheta)d\vartheta=2\pi\frac{y_0+y_1+\cdots+y_n}{n+1}.$$

L. FEJÉR has stated without proof[1]) that this property for the point-system ϑ_k^* is characteristic. More precisely, the following statement holds:

Let

$$\vartheta_0<\vartheta_1<\cdots<\vartheta_n<\vartheta_0+2\pi,$$

and suppose that for any trigonometric polynomial $\varphi(\vartheta)$ of order $\leqq n$ with real coefficients, the conditions

$$\varphi(\vartheta_0)=0,\ \varphi(\vartheta_1)=0,\ \ldots,\ \varphi(\vartheta_n)=0$$

[1]) See L. FEJÉR, Über Interpolation, *Nachrichten der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse*, **1916**, 66—91, in particular p. 91.

imply $\int_0^{2\pi} \varphi(\vartheta)d\vartheta = 0$. *Then we have necessarily*

$$\vartheta_0 = \tau,\ \vartheta_1 = \tau + \frac{2\pi}{n+1}, \ldots, \vartheta_n = \tau + n\frac{2\pi}{n+1}$$

with some real number τ.

Let us be permitted to communicate here an easy proof for this theorem of FEJÉR.

Consider the polynomial

$$g(z) = (z-z_0)(z-z_1)\cdots(z-z_n) = z^{n+1} + a_1 z^n + \cdots + a_{\nu+1} z^{n-\nu} + \cdots + a_{n+1},$$

where

$$z_k = \cos\vartheta_k + i\sin\vartheta_k \qquad (k = 0, 1, \ldots, n),$$

and put

$$g_\nu(z) = z^{\nu-n} g(z) \qquad (\nu = 0, 1, \ldots, n-1).$$

Then $\chi_\nu(\vartheta) = g_\nu(\cos\vartheta + i\sin\vartheta)$ is a trigonometric polynomial of order $\leqq n$ with the absolute member $a_{\nu+1}$. Let $\varphi_\nu(\vartheta)$ and $\psi_\nu(\vartheta)$ be the real and imaginary parts of $\chi_\nu(\vartheta)$, these are trigonometric polynomials of order n at most with real coefficients. Since $\chi_\nu(\vartheta_k) = z_k^{\nu-n} g(z_k) = 0$, thus

$$\varphi_\nu(\vartheta_k) = 0,\ \psi_\nu(\vartheta_k) = 0 \qquad (k = 0, 1, \ldots, n),$$

so we have by assumption

$$\int_0^{2\pi} \varphi_\nu(\vartheta)d\vartheta = 0,\ \int_0^{2\pi} \psi_\nu(\vartheta)d\vartheta = 0,$$

i. e. the polynomials $\varphi_\nu(\vartheta)$, $\psi_\nu(\vartheta)$ have their absolute members equal to zero. Thus we have

$$a_{\nu+1} = 0 \qquad (\nu = 0, 1, \ldots, n-1),$$

i. e.

$$g(z) \equiv z^{n+1} + a_{n+1}.$$

Consequently the roots of $g(z)$ form a regular $(n+1)$-angle inscribed in the unit circle. This proves the theorem.

(Received November 30, 1959)

Über die Szépschen Ringerweiterungen

Von J. SZENDREI in Szeged

Herrn Prof. L. Rédei zum 60. Geburtstag gewidmet

1.

J. SZÉP hat in seiner Arbeit [8] den Begriff der allgemeinen Zerlegung eines Ringes eingeführt und das entsprechende inverse Erweiterungsproblem für zwei Ringe gelöst. Es handelt sich um die ringtheoretischen Analoga der faktorisierbaren Gruppen bzw. des Zappa—Szépschen Produktes von zwei Gruppen. Es ergaben sich gewisse Resultate allgemeiner Natur über diese Ringerweiterungen, die man als die ringtheoretischen Analoga von gruppentheoretischen Sätze [2, 6, 7] betrachten kann.

Wir werden hier zeigen, daß man Sätze bekommen kann, die eine „stärkere" Ähnlichkeit mit Sätzen aus der Theorie der Gruppenfaktorisation aufweisen, wenn die von L. RÉDEI [3, 4] eingeführte Doppelendomorphismen, und (befreundeten) Doppelhomothetismen statt der (einseitigen) Endomorphismen als Hilfsmittel verwendet werden.[1]) Ferner werden wir auf diese Weise weitere Sätze über die Szépschen Ringerweiterungen gewinnen.

2.

Zunächst werden wir einige bekannte, grundlegende Begriffe und Formeln zusammenfassen um uns leichter auf sie beziehen zu können. (Vgl. L. RÉDEI [3, 4] und J. SZÉP [8].)

Wir bezeichnen einen (assoziativen) Ring mit R und die Elemente von R mit $o, a, b, \ldots$. Für eine *Doppelabbildung* A von R in sich bezeichnet man mit ${}^{\mathsf{A}}a, a^{\mathsf{A}}$ die entsprechenden Bilder von a, so daß dann A aus den zwei Abbildungen

$$a \to {}^{\mathsf{A}}a, \quad a \to a^{\mathsf{A}} \qquad (a \in R)$$

[1]) Diese Begriffe wurden von G. HOCHSCHILD in seiner Arbeit [1] schon früher eingeführt, doch werden wir die Arbeiten [3, 4] von L. RÉDEI zitieren, weil hier die von ihm herrührende Terminologie gebraucht wird.

besteht (in dieser Reihenfolge). Unter der trivialen Doppelabbildung von R in sich versteht man diejenige, bei der alle Bildelemente gleich o sind. In der Menge der Doppelabbildungen von R in sich definiert man die Summe und das Produkt von zwei Doppelabbildungen A, B folgendermaßen:

$$(1) \qquad {}^{\mathsf{A}+\mathsf{B}}a = {}^{\mathsf{A}}a + {}^{\mathsf{B}}a, \quad a^{\mathsf{A}+\mathsf{B}} = a^{\mathsf{A}} + a^{\mathsf{B}},$$

$$(2) \qquad {}^{\mathsf{A}\mathsf{B}}a = {}^{\mathsf{A}}({}^{\mathsf{B}}a), \quad a^{\mathsf{A}\mathsf{B}} = (a^{\mathsf{A}})^{\mathsf{B}}.$$

Ein *Doppelhomothetismus* von R bedeutet eine Doppelabbildung A von R in sich mit den Eigenschaften:

$$(3) \qquad {}^{\mathsf{A}}(a+b) = {}^{\mathsf{A}}a + {}^{\mathsf{A}}b, \quad (a+b)^{\mathsf{A}} = a^{\mathsf{A}} + b^{\mathsf{A}},$$

$$(4) \qquad {}^{\mathsf{A}}(ab) = ({}^{\mathsf{A}}a)b, \quad (ab)^{\mathsf{A}} = a(b^{\mathsf{A}}),$$

$$(5) \qquad a({}^{\mathsf{A}}b) = (a^{\mathsf{A}})b,$$

$$(6_0) \qquad ({}^{\mathsf{A}}a)^{\mathsf{A}} = {}^{\mathsf{A}}(a^{\mathsf{A}}).$$

Ein beliebiger Ring D von *befreundeten Doppelhomothetismen* von R ist ein Ring von Doppelabbildungen von R in sich, für die außer den Eigenschaften (1)—(5)

$$(6) \qquad ({}^{\mathsf{A}}a)^{\mathsf{B}} = {}^{\mathsf{A}}(a^{\mathsf{B}})$$

für alle $\mathsf{A}, \mathsf{B} \in D$ erfüllt ist. Es ist klar, daß (6_0) in (6) enthalten ist. Nach L. RÉDEI ist der folgende Satz bekannt:

Jeder Ring D von befreundeten Doppelhomothetismen von R ist mindestens in einem solchen maximalen Ring enthalten.

Sei ein anderer Ring P mit den Elementen $0, \alpha, \beta, \ldots$ gegeben. Das Szépsche Erweiterungsproblem besteht darin, aus den gegebenen Ringen R, P alle Ringe $\mathfrak{R}$ mit[2])

$$\mathfrak{R}^+ = \mathfrak{S}_1^+ \dot{+} \mathfrak{S}_2^+, \quad \mathfrak{S}_1 \approx R, \quad \mathfrak{S}_2 \approx \mathsf{P}, \quad \mathfrak{S}_1 \cap \mathfrak{S}_2 = 0$$

zu bestimmen, wobei $\mathfrak{S}_1, \mathfrak{S}_2$ Unterringe von $\mathfrak{R}$ sind. Die Lösung dieses Problems gewinnt man auf folgende Weise:[3]) In der Menge $\mathfrak{R} = R \cdot \mathsf{P}$ der (geordneten) Paare (a, α) $(a \in R, \alpha \in \mathsf{P})$ definieren wir die Gleichheit, die Addition und die Multiplikation durch die folgenden Relationen:

$$(a, \alpha) = (b, \beta) \Longleftrightarrow a = b, \alpha = \beta,$$

$$(A) \qquad (a, \alpha) + (b, \beta) = (a + b, \alpha + \beta),$$

$$(B) \qquad (a, \alpha)(b, \beta) = (ab + {}^{\alpha}b + a^{\beta}, {}^{\alpha}\beta + \alpha^{b} + \alpha\beta),$$

---

[2]) $\dot{+}$ bezeichnet die direkte Summe von Moduln, durch das oben angesetzten „+" Zeichen wird der Modul des Ringes bezeichnet und $\approx$ ist das Zeichen des Isomorphismus.

[3]) Vgl [5].

wobei die Funktionen

(C) $$ {}^{\alpha}a,\ a^{\alpha} \in R, \quad {}^{\alpha}\alpha,\ \alpha^{\alpha} \in \mathsf{P} $$

den „Anfangsbedingungen"

(D) $$ {}^{\alpha}o = o^{\alpha} = {}^{0}a = a^{0} = o, \quad {}^{\alpha}0 = 0^{\alpha} = {}^{0}\alpha = \alpha^{0} = 0 $$

unterworfen sind. Die soeben definierte Struktur $\mathfrak{R}$ ist dann und nur dann ein Ring, wenn

(1*) $$ {}^{\alpha+\beta}a = {}^{\alpha}a + {}^{\beta}a, \quad a^{\alpha+\beta} = a^{\alpha} + a^{\beta}, $$

(2*) $$ {}^{\alpha\beta}a = {}^{\alpha}({}^{\beta}a), \quad a^{\alpha\beta} = (a^{\alpha})^{\beta}, $$

(3*) $$ {}^{\alpha}(a+b) = {}^{\alpha}a + {}^{\alpha}b, \quad (a+b)^{\alpha} = a^{\alpha} + b^{\alpha}, $$

(4*) $$ {}^{\alpha}(ab) = ({}^{\alpha}a)b + {}^{\alpha^{a}}b, \quad (ab)^{\alpha} = a(b^{\alpha}) + a^{{}^{a}\alpha}, $$

(5*) $$ a({}^{\alpha}b) + a^{({}^{\alpha}b)} = (a^{\alpha})b + {}^{({}^{a}\alpha)}b, $$

(6*) $$ ({}^{\alpha}a)^{\beta} = {}^{\alpha}(a^{\beta}) $$

und die dualen Gleichungen[4]) gelten. Diese Ringe sind bis auf Isomorphie die sämtlichen *Szépschen Erweiterungen* $\mathfrak{R}$ von R und P. $(R, 0)$ und (o, P) sind Unterringe[5]) von $\mathfrak{R}$ und

$$ \mathfrak{R}^{+} = (R, 0)^{+} \dotplus (o, \mathsf{P})^{+}, \quad (R, 0) \approx R\ ((a, 0) \to a), \quad (o, \mathsf{P}) \approx \mathsf{P}\ ((o, \alpha) \to \alpha). $$

3.

Wir legen uns eine Erweiterung $\mathfrak{R}$ von R und P in dem besprochenen Sinne vor. Anders gesagt bedeutet das, daß wir vier Funktionen ${}^{\alpha}a,\ a^{\alpha} (\in R)$, ${}^{\alpha}\alpha,\ \alpha^{\alpha} (\in \mathsf{P})$ mit (D) und (1*)—(6*) vorgeben. Diese Funktionen kann man als Operatorprodukte auffassen. In diesem Sinne ist z. B. P gleichzeitig ein Rechts- und Linksoperatorbereich von R. Daraus folgt, daß jedes Element α von P eine Doppelabbildung $a \to {}^{\alpha}a,\ a \to a^{\alpha}$ von R in sich mit den Eigenschaften (D), (1*)—(6*) induziert. Diese durch α induzierte Doppelabbildung von R in sich bezeichnen wir mit α^{*} und die Menge von α^{*} mit P^{*}. Aus (3) folgt, daß jede Doppelabbildung α^{*} ein Doppelendomorphismus von R^{+}, aber wegen

[4]) Es ist leicht zu sehen, daß die Vertauschung der lateinischen und griechischen Buchstaben in einer gültigen Formel in R wegen (A) und (B) eine richtige Formel in P liefert, die die *duale* der ursprünglichen Formel genannt wird. Von je zwei zueinander dualen Behauptungen, Formeln oder Definitionen genügt es also, immer nur die eine zu beweisen bzw. zu erklären.

[5]) Sind K, K Komplexe von R bzw. P, so soll (K, K) stets den Komplex derjenigen Elemente (a, α) bezeichnen, für die $a \in K$, $\alpha \in \mathsf{K}$ gelten.

(4*) und (5*) im allgemeinen kein Doppelhomothetismus von R ist. Zur näheren Untersuchung des Ringes R können diese Doppelabbildungen gute Dienste leisten. Für die Addition und Multiplikation dieser Doppelabbildungen gelten nach (1*), (2*)

$$\alpha^* + \beta^* = (\alpha + \beta)^*,$$

$$\alpha^* \beta^* = (\alpha\beta)^*.$$

Hieraus und aus (1*)—(6*) kann man leicht beweisen, daß P^* einen zu P homomorphen Ring bildet: d. h.

$$\mathsf{P} \sim \mathsf{P}^* \quad (\alpha \to \alpha^*). \tag{7}$$

Also besteht die homomorphe Abbildung einfach darin, daß man jedes Ringelement α der durch α induzierten Doppelabbildung α^* zuordnet. Bezeichnen wir den Kern des Homomorphismus (7) mit $\mathsf{K}(\mathsf{P})$; d. h. $\mathsf{K}(\mathsf{P})$ ist die Menge der α mit ${}^{\alpha}a = a^{\alpha} = o$ für alle $a \in R$. $\mathsf{K}(\mathsf{P})$ ist also ein (zweiseitiges) Ideal in P. Man kann $\mathsf{K}(\mathsf{P})$ kurz den *Ring der trivialen Doppelabbildungen* in P nennen.

Wir werden im folgenden nur diejenigen Elemente ϱ von P betrachten, für die

$$ {}^{\varrho}a = a^{\varrho} = a^{(\varrho^b)} = o \tag{8}$$

für alle $a, b \in R$ erfüllt ist. Wir bezeichnen die Menge dieser ϱ mit P_0. Es gilt offenbar $\mathsf{P}_0 \subseteqq \mathsf{K}(\mathsf{P})$. Sind $\varrho, \sigma \in \mathsf{P}_0$ und $\alpha \in \mathsf{P}$, so folgen die Gleichungen

$$ {}^{\varrho-\sigma}a = a^{\varrho-\sigma} = a^{({}^{(\varrho-\sigma)^a})} = o, \quad {}^{\alpha\varrho}a = a^{\alpha\varrho} = o$$

unmittelbar aus (1*) bzw. (2*). Ferner ergibt sich aus (4*), (1*) wegen der Annahme (8)

$$a^{(({}^{\alpha}\varrho)^b)} = a^{(\alpha(\varrho^b) + {}^{\alpha}\varrho^b)} = (a^{\alpha})^{(\varrho^b)} + a^{({}^{\alpha}\varrho^b)} = o.$$

Ganz ähnlich sieht man ein, daß $a^{({}^{(\varrho\alpha)}b)} = o$. Somit haben wir bewiesen, daß P_0 ein Ideal in P ist.

Zulässig nennen wir einen Unterring T von P, wenn ${}^{a}\tau, \tau^{a} \in \mathsf{T}$ für alle $\tau \in \mathsf{T}$, $a \in R$ erfüllt ist.

4.

Nach dieser Vorbereitung beweisen wir den folgenden

Satz 1. *Wenn die Funktionen* (C) *mit den Bedingungen* (D), (1*)—(6*) *für die Ringe* R, P *definiert sind, dann sind* R_0, P_0 *zulässige Ideale von* R

bzw. P, *ferner sind* R *und* P *je ein Bereich*[6]) *befreundeter Doppelhomothetismen für* P_0 *bzw.* R_0.[7])

Beweis. Wir betrachten den Unterring P_0, der nach dem obigen ein Ideal von P ist. Es ist zu beweisen, daß ${}^a\varrho, \varrho^a \in \mathsf{P}_0$ für alle $a \in R$, $\varrho \in \mathsf{P}_0$ gilt. Wegen (8) folgt aus (4*) und (5*)

$$({}^a\varrho)b = b^{({}^a\varrho)} = ({}^{\varrho^a})b = b^{(\varrho^a)} = o,$$

ferner ergibt sich wegen der Annahme aus der zu (6*) dualen Relation und aus (4*) bzw. aus der dualen Relation zu (2*)

$$b^{({}^a\varrho)^c} = b^{a(\varrho^c)} = (ba)^{\varrho^c} = b(a^{(\varrho^c)}) = o, \quad b^{(\varrho^a)^c} = b^{(\varrho^{ac})} = o.$$

Damit haben wir bewiesen, daß P_0 ein zulässiges Ideal von P ist. Endlich verschwindet wegen (8) jeder zweite Summand auf der rechten Seite der dualen Gleichungen von (4*) und (5*); deshalb bildet die Menge der Doppelabbildungen $\varrho \to {}^a\varrho$, $\varrho \to \varrho^a$ von P_0 in sich für alle $a \in R$ einen Ring von befreundeten Doppelhomothetismen von P_0. Damit ist Satz 1 bewiesen.

Bemerkung. Der nur durch $\varrho a = a\varrho = o$ (für alle $a \in R$) definierte Unterring von P, d. h. $\mathsf{K}(\mathsf{P})$ ist im allgemeinen nicht zulässig, wie das folgende Beispiel zeigt. Sei $\mathfrak{R}$ der volle Matrixring vom Rang 2^2 über dem Ring der ganzen rationalen Zahlen; R bzw. P bezeichnen den Unterring der Elemente von der Form $a = \begin{pmatrix} 0 & 0 \\ w & 0 \end{pmatrix}$ bzw. $\alpha = \begin{pmatrix} u & v \\ 0 & z \end{pmatrix}$. Es ist klar, daß $\mathfrak{R}$ eine Szépsche Erweiterung von R und P ist. Die Funktionen werden auf folgende Weise definiert:

$${}^a a = \begin{pmatrix} 0 & 0 \\ wz & 0 \end{pmatrix}, \quad a^a = \begin{pmatrix} 0 & 0 \\ wu & 0 \end{pmatrix}, \quad {}^\alpha a = \begin{pmatrix} 0 & 0 \\ 0 & wv \end{pmatrix}, \quad \alpha^a = \begin{pmatrix} vw & 0 \\ 0 & 0 \end{pmatrix}.$$

Offenbar ist $\varrho = \begin{pmatrix} 0 & v \\ 0 & 0 \end{pmatrix}$ in $\mathsf{K}(\mathsf{P})$ enthalten, doch liegen die Elemente ${}^\varrho = \begin{pmatrix} 0 & 0 \\ 0 & wv \end{pmatrix}$, $\varrho^\alpha = \begin{pmatrix} vw & 0 \\ 0 & 0 \end{pmatrix}$ nicht in $\mathsf{K}(\mathsf{P})$.

Für R_0 und P_0 gilt der folgende

Satz 2. *In einer Erweiterung* $\mathfrak{R}$ *von* R *und* P *ist* $(R_0, 0)$ *bzw.* (o, P_0) *je das größte in* $(R, 0)$ *bzw.* (o, P) *enthaltene Ideal. Ferner ist* (R_0, P_0) *ein Ideal*

---

[6]) D. h. die durch die Elemente von R induzierten Doppelabbildungen $\varrho_0 \to {}^a\varrho_0$, $\varrho_0 \to \varrho_0^a$ $(a \in R, \varrho_0 \in \mathsf{P}_0)$ von P_0 in sich einen Ring von befreundeten Doppelhomothetismen von P_0 bilden.

[7]) Den analogen Satz für Gruppen siehe z. B. in [2] (Satz 7).

in $\mathfrak{R}$, *und es gilt*[8])[9])

$$(R_0, \mathsf{P}_0) = (R_0, 0) \oplus (o, \mathsf{P}).$$

Beweis. Es ist leicht zu sehen, daß (o, P_0) ein Ideal von $\mathfrak{R}$ ist. Nehmen wir nun umgekehrt an, daß (o, T) ein Ideal von $\mathfrak{R}$ ist. Da die Produkte $(a, 0)(o, \tau) = (a^\tau, {}^a\tau)$ und $(o, \tau)(a, 0) = ({}^\tau a, \tau^a)$ für alle $a \in R$ und $\tau \in \mathsf{T}$ in (o, T) enthalten sind, folgt ${}^\tau a = a^\tau = o$. Aus $(a, 0)((o, \tau)(b, 0)) = (a^{({}^\tau b)}, {}^a({}^\tau b)) \in (o, \mathsf{T})$ ergibt sich ferner $a^{({}^\tau b)} = o$ für $a, b \in R$ und $\tau \in \mathsf{T}$, d. h. $\mathsf{T} \subseteq \mathsf{P}_0$. Daher ist (o, P_0) das größte in (o, P) enthaltene Ideal von $\mathfrak{R}$. $(\mathfrak{R}_0, \mathsf{P}_0)$ ist offenbar ein Ideal in $\mathfrak{R}$. Da das Nullelement $(o, 0)$ das einzige gemeinsame Element von $(R_0, 0)$ und (o, P_0) ist, folgt daraus die Richtigkeit der Behauptung in Satz 2.

Falls die Erweiterung $\mathfrak{R}$ einfach ist, leistet der folgende Satz gute Dienste:

Satz 3. *Ist die Erweiterung* $\mathfrak{R}$ *von* R *und* P *einfach, so kann keiner der Ringe* R, P *ein Bereich befreundeter Doppelhomothetismen für den anderen sein.*[10])

Beweis. Um den Satz zu beweisen, nehmen wir an, daß P ein Bereich befreundeter Doppelhomothetismen für R ist. Dies bedeutet, daß

$$({}^{b\alpha})a = a^{({}^{b\alpha})} = ({}^{\alpha b})a = a^{(\alpha^b)} = o$$

für alle $a, b \in R$, $\alpha \in \mathsf{P}$ gilt. Daraus folgt aber $a^{({}^{b\alpha})^c} = o$, $a^{(\alpha^b)^c} = o$, d. h. ${}^{b\alpha} = \alpha^b \in \mathsf{P}_0$ für alle $b \in R$, $\alpha \in \mathsf{P}$. Nach Satz 2 muß $\mathsf{P}_0 = o$ sein, folglich gilt

$${}^{b\alpha} = \alpha^b = \alpha^{({}^b\beta)} = 0$$

für jedes $b \in R$, $\alpha, \beta \in \mathsf{P}$. Dies besagt wegen (8), daß $R = R_0$. Nach Satz 2 ergibt sich, daß (R, o) ein Ideal von $\mathfrak{R}$ ist. Das ist ein Widerspruch zur Voraussetzung und hiermit ist Satz 3 bewiesen.

Wir beweisen nun den folgenden

Satz 4. *Wenn jeder der Ringe* R, P *in* $\mathfrak{R}$ *ein Bereich befreundeter Doppelhomothetismen für den anderen ist, dann gilt*[11])

$$\mathfrak{R}/(R_0, \mathsf{P}_0) \approx R/R_0 \oplus \mathsf{P}/\mathsf{P}_0.$$

Beweis. Die Annahme bedeutet genau, daß z. B. ${}^a\alpha, \alpha^a \in \mathsf{P}_0$ für alle $a \in R$, $\alpha \in \mathsf{P}$ gilt, wie wir das oben schon gesehen haben. Daraus folgt, daß (R_0, P) und (R, P_0) Ideale in $\mathfrak{R}$ sind, die nach Satz 2 den Unterring (R_0, P_0) als Ideal enthalten. Deshalb sind die Faktorringe $(R_0, \mathsf{P})/(R_0, \mathsf{P}_0)$ und $(R, \mathsf{P}_0)/(R_0, \mathsf{P}_0)$

[8]) Mit $\oplus$ bezeichnen wir die direkte Summe von Ringen im ringtheoretischen Sinne.
[9]) Den entsprechenden Satz im Fall der Gruppen siehe z. B. in [2] (Satz 8).
[10]) Den entsprechenden gruppentheoretischen Satz siehe z. B. in [2] (Satz 10).
[11]) Den analogen Satz für Gruppen siehe z. B. in [2] (Satz 11).

Ideale von $\mathfrak{R}/(R_0, P_0)$. Ferner ist klar, daß diese Faktorringe (Ideale) kein Element außer (R_0, P_0) gemeinsam haben und jedes Element von $\mathfrak{R}/(R_0, P_0)$ als Summe von Elementen aus $(R, P_0)/(R_0, P_0)$ und $(R_0, P)/(R_0, P_0)$ darstellbar ist. Dies bedeutet eben, daß

$$\mathfrak{R}/(R_0, P_0) = (R, P_0)/(R_0, P_0) \oplus (R_0, P)/(R_0, P_0).$$

Hieraus ergibt sich wegen

$$(R, P_0)/(R_0, P_0) \approx R/R_0, \quad (R_0, P)/(R_0, P_0) \approx P/P_0$$

die Richtigkeit der Behauptung. Somit ist Satz 4 bewiesen.

Literaturverzeichnis

[1] G. Hochschild, On the cohomology theory for associative algebras, *Annals of Math.*, **47** (1946), 568—579.
[2] L. Rédei, Die Anwendung des schiefen Produktes in der Gruppentheorie, *Journal für die reine und angewandte Math.*, **188** (1950), 201—227.
[3] L. Rédei, Die Holomorphentheorie für Gruppen und Ringe, *Acta Math. Acad. Sci. Hung.*, **5** (1954), 169—195.
[4] L. Rédei, *Algebra* I (Leipzig, 1959).
[5] J. Szendrei, Über eine allgemeine Ringkonstruktion durch schiefes Produkt, *Acta Sci. Math.*, **19** (1958), 63—76.
[6] J. Szép, Über die als Produkt zweier Untergruppen darstellbaren endlichen Gruppen, *Commentarii Math. Helvetici*, **22** (1949), 31—33.
[7] J. Szép, On the structure of groups which can be represented as the product of two subgroups, *Acta Sci. Math.*, **12A** (1950), 57—61.
[8] J. Szép, Über eine neue Erweiterung von Ringen. I, *Acta Sci. Math.*, **19** (1958), 51—62.

(Eingegangen am 24. Dezember 1959)

Les points exceptionnels sur les cubiques $ax^3+by^3+cz^3=0$

Par T. NAGELL à Uppsala (Suède)

Dédié au 60ième anniversaire de mon ami Ladislaus Rédei

1. Dans un travail qui vient de paraître dans les *Acta Arithmetica*[1]), j'ai établi entre autres le résultat suivant:

Théorème I. *Soit Ω un corps algébrique dans lequel le nombre des classes d'idéaux est égal à 1. Considérons la cubique*

$$ax^3+by^3+cz^3=0, \tag{1}$$

où les coefficients a, b et c sont des nombres, différents de zéro, dans Ω. Deux cubiques de la forme (1) *sont considérées comme identiques quand elles sont linéairement équivalentes dans Ω. Désignons par m le nombre des points exceptionnels dans Ω sur la cubique.*

Supposons d'abord que Ω ne contient pas le nombre $\sqrt{-3}$. Si la relation

$$1+E+E_1=0 \tag{2}$$

est impossible ou si elle est satisfaite par une seule paire d'unités E et E_1 dans Ω, on a $m=0$, sauf dans les cas suivants: Si la cubique a la forme

$$x^3+y^3+cz^3=0, \tag{3}$$

où ni c ni 4c n'est égal à un cube dans Ω, on a $m=1$. Si la cubique a la forme

$$x^3+y^3+2z^3=0, \tag{4}$$

et si le nombre 2 n'est pas égal à un cube dans Ω, on a $m=2$. Enfin, pour la cubique

$$x^3+y^3+z^3=0 \tag{5}$$

[1]) T. NAGELL, Les points exceptionnels rationnels sur certaines cubiques du premier genre, *Acta Arithmetica*, **5** (1959), 333—357. A propos de l'explication des notions nous renvoyons le lecteur à ce travail.

on a $m=6$ *ou* $m=3$, *selon que le nombre* 2 *est égal à un cube dans* Ω *ou non.*

Supposons ensuite que Ω *contient le nombre* $\sqrt{-3}$. *Alors on a* $m=0$ *si la relation* (2) *n'est satisfaite que par la paire d'unités* $\varrho=\frac{1}{2}(-1+\sqrt{-3})$ *et* $\varrho^2=\frac{1}{2}(-1-\sqrt{-3})$ *dans* Ω, *exception faite des cas suivants: Pour la cubique* (3) *on a* $m=3$. *Pour la cubique* (4) *on a* $m=12$. *Pour la cubique* (5) *on a* $m=9$. *Pour la cubique*

$$x^3+\varrho y^3+\varrho^2 z^3=0 \tag{6}$$

on a $m=9$.

Ce théorème est vrai par exemple quand Ω *est un corps quadratique simple ou un corps cubique simple à discriminant négatif.*

2. Dans le présent travail nous allons traiter du cas d'un corps algébrique Ω dans lequel le nombre des classes d'idéaux est plus grand que l'unité. Cependant, pour obtenir un résultat analogue au Théorème I dans ce cas nous sommes forcés à faire certaines suppositions restrictives sur les coefficients a, b et c de la cubique (1).

Nous supposons que les coefficients satisfont aux conditions suivantes:

a, b et c sont des nombres entiers dans Ω, *différents de zéro. Aucun des idéaux principaux* (a), (b), (c) *n'est divisible par le cube d'un idéal premier. Les idéaux* (a), (b) *et* (c) *sont premiers entre eux deux à deux.*

Deux cubiques de la forme (1) sont considérées comme identiques quand elles sont reliées par des transformations linéaires appartenant à Ω.

3. Soit $P=P(x, y, z)$ un point rationnel dans Ω sur la cubique (1), c'est-à-dire que les coordonnées x, y, z sont proportionnelles à trois nombres dans Ω. Désignons par

$$(x, y, z)=\mathfrak{j} \tag{7}$$

le plus grand commun diviseur des idéaux (x), (y) et (z). Alors on a

$$\left(\frac{x}{\mathfrak{j}}, \frac{y}{\mathfrak{j}}\right)=\left(\frac{x}{\mathfrak{j}}, \frac{z}{\mathfrak{j}}\right)=\left(\frac{y}{\mathfrak{j}}, \frac{z}{\mathfrak{j}}\right)=1. \tag{8}$$

En effet, soit $\mathfrak{p}$ un idéal premier qui divise l'un et l'autre des deux idéaux $\left(\frac{x}{\mathfrak{j}}\right)$ et $\left(\frac{y}{\mathfrak{j}}\right)$. Alors il suit de l'équation (1) que

$$c\cdot\left(\frac{z}{\mathfrak{j}}\right)^3\equiv 0 \pmod{\mathfrak{p}^3}.$$

Or, d'après l'hypothése faite sur les coefficients, c n'est pas divisible par le cube $\mathfrak{p}^3$. Donc on aura

$$\left(\frac{z}{\mathfrak{j}}\right)\equiv 0 \pmod{\mathfrak{p}}.$$

Il en résulterait que l'idéal $\left(\frac{x}{\mathfrak{j}}, \frac{y}{\mathfrak{j}}, \frac{z}{\mathfrak{j}}\right)$ serait divisible par $\mathfrak{p}$. Or, cela serait en contradiction avec (7). Donc, les relations (8) sont vraies.

Si $N(\mathfrak{A})$ signifie la norme de l'idéal $\mathfrak{A}$ dans Ω, nous appelons le nombre

$$N\left(\frac{xyz}{\mathfrak{j}^3}\right) \tag{9}$$

l'index du point $P(x, y, z)$. L'index est un nombre entier positif dans $\mathbf{K}(1)$, sauf quand P est un point d'inflexion; l'index d'un point d'inflexion est évidemment $=0$.

4. Désignons par $P_1 = P_1(\xi, \eta, \zeta)$ le point tangentiel du point $P=P(x, y, z)$. Les coordonées ξ, η et ζ de P_1 sont alors données par les formules

$$\begin{cases} \xi = x(by^3 - cz^3), \\ \eta = y(cz^3 - ax^3), \\ \zeta = z(ax^3 - by^3). \end{cases} \tag{10}$$

Il résulte de là que ξ, η et ζ sont tous les trois divisibles par $\mathfrak{j}^4$. Soit $\mathfrak{A}$ un idéal tel qu'on ait

$$\left(\left(\frac{\xi}{\mathfrak{j}^4}\right), \left(\frac{\eta}{\mathfrak{j}^4}\right), \left(\frac{\zeta}{\mathfrak{j}^4}\right)\right) = \mathfrak{A}. \tag{11}$$

Soit $\mathfrak{p}$ un idéal premier qui divise $\mathfrak{A}$. Supposons que $\left(\frac{x}{\mathfrak{j}}\right)$ soit divisible par $\mathfrak{p}$. On déduit alors de la seconde équation dans (10)

$$\left(\frac{y}{\mathfrak{j}}\right)\left(\frac{cz^3 - ax^3}{\mathfrak{j}^3}\right) = \left(\frac{y}{\mathfrak{j}}\right)\left(\frac{-2ax^3 - by^3}{\mathfrak{j}^3}\right) \equiv 0 \pmod{\mathfrak{p}},$$

donc

$$b\left(\frac{y}{\mathfrak{j}}\right) \equiv 0 \pmod{\mathfrak{p}}, \tag{12}$$

et on déduit de la troisième équation dans (10)

$$\left(\frac{z}{\mathfrak{j}}\right)\left(\frac{ax^3 - by^3}{\mathfrak{j}^3}\right) = \left(\frac{z}{\mathfrak{j}}\right)\left(\frac{2ax^3 + cz^3}{\mathfrak{j}^3}\right) \equiv 0 \pmod{\mathfrak{p}},$$

donc

$$c\left(\frac{z}{\mathfrak{j}}\right) \equiv 0 \pmod{\mathfrak{p}}. \tag{13}$$

Or, les congruences (12) et (13) ne peuvent pas être satisfaites en même temps. Cela se voit aisément à l'aide des relations (8) et de $(b, c) = 1$.

On en conclut qu'aucun des idéaux $\left(\frac{x}{\mathfrak{j}}\right)$, $\left(\frac{y}{\mathfrak{j}}\right)$ et $\left(\frac{z}{\mathfrak{j}}\right)$ n'est divisible par $\mathfrak{p}$. Donc, tous ces idéaux sont premiers à $\mathfrak{A}$. Il résulte alors de (10) que

$$by^3 - cz^3 \equiv cz^3 - ax^3 \equiv ax^3 - by^3 \equiv 0 \pmod{\mathfrak{A}\mathfrak{p}^3}. \tag{14}$$

On en déduit aisément

$$3a\left(\frac{x}{\mathfrak{j}}\right)^3 \equiv 3b\left(\frac{y}{\mathfrak{j}}\right)^3 \equiv 3c\left(\frac{z}{\mathfrak{j}}\right)^3 \equiv 0 \pmod{\mathfrak{A}}.$$

Vu que $(a, b) = (a, c) = b, c) = \left(\frac{x}{\mathfrak{j}}, \mathfrak{A}\right) = \left(\frac{y}{\mathfrak{j}}, \mathfrak{A}\right) = \left(\frac{z}{\mathfrak{j}}, \mathfrak{A}\right) = 1$, on en conclut que

$$3 \equiv 0 \pmod{\mathfrak{A}}. \tag{15}$$

5. Supposons maintenant que ni P ni P_1 n'est un point d'inflexion. Alors tous les nombres

$$x, y, z, \xi, \eta, \zeta, by^3 - cz^3, cz^3 - ax^3, ax^3 - by^3$$

sont différents de zéro.

Supposons que P est un point exceptionnel dans Ω. Vu que le nombre des points exceptionnels dans Ω est limité, les indices de ces points a un certain maximum M. Supposons que

$$\text{Index } P = N\left(\frac{xyz}{\mathfrak{j}^3}\right) = M.$$

Alors on a

$$\text{Index } P_1 = N\left(\frac{\xi\eta\zeta}{\mathfrak{j}^{12}\mathfrak{A}^3}\right) \leqq M.$$

D'autre part il résulte de (10) et (14) que

$$N\left(\frac{\xi\eta\zeta}{\mathfrak{j}^{12}\mathfrak{A}^3}\right) \geqq N\left(\frac{xyz}{\mathfrak{j}^3}\right).$$

Nous aurons donc

$$\text{Index } P_1 = \text{Index } P = M,$$

et par conséquent:

$$(by^3 - cz^3) = (cz^3 - ax^3) = (ax^3 - by^3) = \mathfrak{A}\mathfrak{j}^3. \tag{16}$$

Ces relations entraînent

$$cz^3 - ax^3 = E(by^3 - cz^3),$$
$$ax^3 - by^3 = E_1(by^3 - cz^3),$$

où E et E_1 sont des unités dans Ω, qui satisfont à l'équation

$$1+E+E_1=0. \tag{17}$$

6. De ce qui précède nous aurons le résultat suivant:

Théorème II. *Soit Ω un corps algébrique qui ne contient pas le nombre $\sqrt{-3}$. Soit donnée la cubique*

$$ax^3+by^3+cz^3=0,$$

où les coefficients a, b et c sont des nombres entiers dans Ω qui satisfont aux conditions suivantes: Les idéaux principaux (a), (b) et (c) sont premiers entre eux deux à deux, et aucun d'eux n'est divisible par le cube d'un idéal premier.

Désignons par m le nombre des points exceptionnels dans Ω sur la cubique. Si la relation (17) *n'est satisfaite par aucune paire d'unités E et E_1 dans Ω, on a $m=0$, sauf dans les cas suivants: Si la cubique a la forme*

$$x^3+y^3+cz^3=0, \tag{18}$$

où ni c ni 4c n'est égal au cube d'un nombre dans Ω, on a $m=1$. Si la cubique a la forme

$$x^3+y^3+2z^3=0, \tag{19}$$

on a $m=2$.[1]) *Si la cubique a la forme*

$$x^3+y^3+z^3=0, \tag{20}$$

on a $m=3$.

Les cubiques d'exception (18), (19) et (20) représentent, tout comme au Théorème I, les cas dans lesquels un seul ou plusieurs points d'inflexion appartiennent à Ω.

Théorème II est vrai quand Ω est un corps quadratique ou un corps cubique à discriminant négatif. En effet, dans mon travail précité, j'ai montré que la relation (17) n'est pas satisfaite dans ces corps, exception faite d'un nombre fini de corps simples.

7. Les Théorèmes I et II sont encore vrais quand Ω est un corps biquadratique jouissant des propriétés suivantes: Tous les quatre corps conjugués sont imaginaires. Ω est différent des corps engendrés par les cinquièmes, huitièmes et douzièmes racines primitives de l'unité. Ω admet un sous-corps quadratique réel différent de $\mathbf{K}(\sqrt{5})$. Ω ne contient pas le nombre $\sqrt{-3}$.

[1]) Le nombre 2, étant par hypothèse indivisible par le cube d'un idéal premier, ne peut être le cube d'un nombre dans Ω.

En effet, dans ce cas il y a une seule unité fondamentale η dans Ω, telle que toutes les unités du corps soient données sous la forme $\varrho\eta^M$, où ϱ est une racine de l'unité appartenant à Ω, et où M est un nombre entier rationnel. On peut supposer que $|\eta| > 1$, et si η est réel que $\eta > 1$. A cause des restrictions faites sur Ω il ne reste pour ϱ que les possibilités ± 1 et $\pm i$. Ω ne peut contenir qu'un seul sous-corps quadratique réel. Désignons par ε l'unité fondamentale de ce sous-corps; nous pouvons choisir $\varepsilon > 1$. Pour une certaine valeur entière de N on a donc

$$\varepsilon = \varrho\eta^N. \tag{21}$$

Vu que $\varepsilon > 1$ et $|\eta| > 1$ on a $N \geqq 1$.

Supposons d'abord que Ω ne contient pas le nombre i. Alors on a dans (21) $\varrho = \pm 1$. D'après le théorème de CAPELLI, le nombre $(\pm\varepsilon)^{\frac{1}{N}}$ est du $2N$-ième degré. Ainsi, quand η est du quatrième degré, on aura

$$\varepsilon = -\eta^2, \tag{22}$$

et quand η est du second degré, on aura

$$\varepsilon = \eta. \tag{23}$$

Dans le dernier cas toutes les unités sont du second degré, et la relation (17) est impossible dans Ω, ainsi que nous l'avons montré dans notre travail précité. Dans le cas (22) la relation (17) est encore impossible quand E et E_1 sont réels et conséquemment du second degré. Si l'unité E est imaginaire, elle est évidemment racine d'une équation de la forme

$$x^4 - ax^2 + 1 = 0,$$

où a est un nombre entier rationnel. Alors E_1 est racine de l'équation

$$(y+1)^4 - a(y+1)^2 + 1 = 0.$$

Comme E_1 et ses conjuguées sont imaginaires, on a nécessairement $a = 1$. Or, les racines de l'équation $x^4 - x^2 + 1 = 0$ sont les douzièmes racines primitives de l'unité.

Supposons ensuite que Ω contient le nombre i. Si dans (21) $\varrho = \pm 1$, on aura comme tout-à-l'heure les possibilités (22) et (23). Or, si $\eta = \sqrt{-\varepsilon}$ le corps ne peut pas contenir le nombre i vu que le produit $-i\sqrt{-\varepsilon} = \sqrt{\varepsilon}$ est un nombre réel du quatrième degré. On a donc $\eta = \varepsilon$. Nous savons déjà que la relation (17) est impossible quand E et E_1 sont du second degré. Soit maintenant E du quatrième degré. Alors le nombre iE est une unité réelle du second degré et racine d'une équation

$$x^2 - ax \pm 1 = 0,$$

où a est un nombre entier rationnel. Alors E est racine de l'équation

$$z^2 + aiz \mp 1 = 0$$

et de l'équation

$$(z^2 \mp 1)^2 + a^2 z^2 = 0.$$

Donc l'unité E_1 est racine de l'équation

$$(y+1)^4 + (y+1)^2(a^2 \mp 2) + 1 = 0.$$

Comme E_1 et ses conjuguées sont imaginaires, on a nécessairement

$$2 + a^2 \mp 2 = 1,$$

d'où il s'ensuit que $a = \pm 1$. Les équations corréspondantes

$$x^2 \mp x \pm 1 = 0$$

sont inadmissibles, vu que Ω ne contient pas les nombres $\sqrt{5}$ et $\sqrt{-3}$.

Supposons finalement que, dans (21), $\varrho = \pm i$. D'après le théorème de CAPELLI, le nombre $(\pm i\varepsilon)^{\frac{1}{N}}$ est ou du $4N$-ième degré ou du $2N$-ième degré. Donc on doit avoir ou $N=2$ ou $N=1$, c'est-à-dire ou $\eta^2 = \pm i\varepsilon$ ou $\eta = \pm i\varepsilon$. Si E et E_1 sont du second degré, on procédera comme tout-à-l'heure. Si E et E_1 sont du quatrième degré, le raisonnement sera le même que dans le cas $\eta = \varepsilon$.

Nous finissons par quelques exemples numériques.

Exemple 1. Soit Ω le corps biquadratique engendré par le nombre $\eta = \sqrt{-2-\sqrt{3}}$, racine de l'équation

$$x^4 + 4x^2 + 1 = 0.$$

Ω est un corps de Galois et contient les trois sous-corps quadratiques $\mathbf{K}(\sqrt{3})$, $\mathbf{K}(\sqrt{-2})$ et $\mathbf{K}(\sqrt{-6})$. L'unité fondamentale dans $\mathbf{K}(\sqrt{3})$ est $\varepsilon = 2+\sqrt{3}$, et η est l'unité fondamentale dans Ω.

Exemple 2. Soit Ω le corps biquadratique engendré par le nombre $\alpha = \sqrt{-3-\sqrt{7}}$, racine de l'équation

$$x^4 + 6x^2 + 2 = 0.$$

Le seul sous-corps quadratique de Ω est $\mathbf{K}(\sqrt{7})$. L'unité fondamentale dans le sous-corps est $\varepsilon = 8+3\sqrt{7}$. Le nombre $\beta = \sqrt{-8-3\sqrt{7}}$ n'appartient pas à Ω. En effet, le quotient $\frac{\alpha}{\beta}$ est égal à $\sqrt{3-\sqrt{7}}$, nombre réel du quatrième degré. Ainsi le nombre $\varepsilon = 8+3\sqrt{7}$ est l'unité fondamentale dans Ω.

Parmi les corps biquadratiques en question il y en a aussi des corps simples, c'est-à-dire des corps dans lesquels le nombre des classes d'idéaux est égal à 1. En effet, les corps de Dirichlet $\mathbf{K}(\sqrt{D}, \sqrt{-D})$ sont simples pour $D = 2, 3, 5, 7, 11, 13, 19, 37, 43, 67, 163$. Dans nos raisonnements plus haut nous avons exclus les cas $D = 2$, 3 et 5. Dans les autres cas Théorème I est vrai.

(Reçu le 13 janvier 1960)

Verallgemeinerung eines graphentheoretischen Satzes von Rédei

Von T. GALLAI in Budapest (Ungarn) und A. N. MILGRAM in Minneapolis (U. S. A.)

Ladislaus Rédei zum 60. Geburtstag

1. Es sei M eine nichtleere endliche Menge, und es bezeichne M_2 die Menge sämtlicher ungeordneter Paare, die man aus *verschiedenen* Elementen von M bilden kann. Die Elemente von M nennen wir *Punkte,* diejenigen von M_2 *Kanten.* Die durch die Punkte P und P' bestimmte Kante wollen wir mit PP' oder $P'P$ bezeichnen und sagen, daß PP' zu den Punkten P und P' *inzident* ist, sowie daß PP' die Punkte P und P' *verbindet.* Es sei N eine beliebige Teilmenge von M_2 ($N \subseteq M_2$). Wir sagen: M und N bestimmen gemeinsam den *Graphen* $\Gamma = (M, N)$. Ist $M_2 = N$, so heißt Γ *vollständig.* Der Ausdruck „P und P' sind *unabhängig* in $\Gamma = (M, N)$" soll bedeuten: $P' \neq P$; $P, P' \in M$; $PP' \notin N$. Die Punkte $P_1, \ldots, P_n$ [1]) *sind unabhängig in* Γ, wenn $P_1, \ldots, P_n$ Punkte von Γ sind und sie im Falle $n > 1$ paarweise unabhängig in Γ sind. Der Ausdruck $p_{\max}(\Gamma)$ soll *die maximale Anzahl der unabhängigen Punkte in* Γ bezeichnen, d. h. $p_{\max}(\Gamma) = k$ bedeutet: es gibt in Γ k unabhängige Punkte, $k+1$ jedoch nicht.

Wir *richten* eine Kante PP' dadurch, daß wir den einen Punkt der Kante als *Anfangspunkt,* den anderen als *Endpunkt* auszeichnen. Je nachdem ob P oder P' der Anfangspunkt ist, soll $\overrightarrow{PP'}$ bzw. $\overrightarrow{P'P}$ das Zeichen der *gerichteten* Kante sein. Richtet man in irgendeiner Weise jede Kante eines Graphen Γ, so entsteht ein *gerichteter* Graph $\vec{\Gamma}$. (Das Zeichen Γ bzw. $\vec{\Gamma}$, auch mit Index versehen, soll immer einen ungerichteten bzw. gerichteten Graphen bedeuten. Einen Graphen, der keine Kante enthält, können wir auch als gerichteten Graphen betrachten.) Sind $P_1, \ldots, P_n$ unabhängig in Γ, so nennen wir sie auch in $\vec{\Gamma}$ unabhängig. Es gilt $p_{\max}(\vec{\Gamma}) = p_{\max}(\Gamma)$.

Enthält $\vec{\Gamma}$ die Kanten $\overrightarrow{P_i P_{i+1}}$ ($i = 1, \ldots, m$), und sind die Punkte $P_1, \ldots, P_{m+1}$ verschieden, so sagen wir, daß diese Kanten eine *Bahn*

[1]) Der Ausdruck $e_m, \ldots, e_n$, wo m und n ganze Zahlen mit $m \leqq n$ bezeichnen, soll im Falle $m = n$ das einzige Element e_m bedeuten.

$b=(P_1,\ldots,P_{m+1})$ von $\vec{\Gamma}$ bilden. Wir wollen auch einen beliebigen Punkt P_1 von $\vec{\Gamma}$ in sich selbst als eine Bahn $b=(P_1)$ von $\vec{\Gamma}$ betrachten. Der Punkt P_1 heißt der Anfangspunkt von $b=(P_1,\ldots,P_{m+1})$ bzw. $b=(P_1)$. Haben die Bahnen $b_1,\ldots,b_n$ von $\vec{\Gamma}$ die Eigenschaft, daß jeder Punkt von $\vec{\Gamma}$ in mindestens einer dieser Bahnen vorkommt, so sagen wir, daß $b_1,\ldots,b_n$ den Graphen $\vec{\Gamma}$ *bedecken*, oder daß das „Bahnsystem" $S=\{b_1,\ldots,b_n\}$ $\vec{\Gamma}$ bedeckt. Die Behauptung „in $\vec{\Gamma}$ ist die minimale Anzahl der bedeckenden Bahnen gleich k" soll bedeuten: Es existieren in $\vec{\Gamma}$ k solche Bahnen, die $\vec{\Gamma}$ bedekken, weniger als k jedoch nicht.

Sind P und P' Punkte von $\vec{\Gamma}$ und existiert in $\vec{\Gamma}$ keine Bahn, die die beiden Punkte P und P' enthält, so sagen wir: P un P' sind *bahnunabhängig* in $\vec{\Gamma}$. $P_1,\ldots,P_n$ sind dann bahnunabhängig in $\vec{\Gamma}$, wenn sie Punkte von $\vec{\Gamma}$ sind und sie im Falle $n>1$ paarweise bahnunabhängig in $\vec{\Gamma}$ sind. „Die maximale Anzahl der bahnunabhängigen Punkte in $\vec{\Gamma}$ ist k" bedeutet: Es gibt in $\vec{\Gamma}$ k solche Punkte, die in $\vec{\Gamma}$ bahnunabhängig sind, $k+1$ jedoch nicht. Sind $P_1,\ldots,P_n$ bahnunabhängig in $\vec{\Gamma}$, so sind sie auch unabhängig in $\vec{\Gamma}$.

Ist $b=(P_1,\ldots,P_n)$ $(n\geqq 3)$ eine Bahn von $\vec{\Gamma}$ und enthält $\vec{\Gamma}$ auch die Kante $\overrightarrow{P_nP_1}$, so bilden die Kanten $\overrightarrow{P_1P_2},\ldots,\overrightarrow{P_{n-1}P_n},\overrightarrow{P_nP_1}$ einen in $\vec{\Gamma}$ liegenden *Kreis*. Enthält der Graph $\vec{\Gamma}$ keinen Kreis, so heißt er *azyklisch*.

Der Graph Γ' ist ein *Teilgraph* von Γ, wenn jeder Punkt und jede Kante von Γ' auch Punkt bzw. Kante von Γ ist. Die gleiche Bedeutung hat die Behauptung, daß $\vec{\Gamma}'$ ein Teilgraph von $\vec{\Gamma}$ ist.

2. Mit den im Abschnitt 1 eingeführten Begriffen kann man nun den im Titel erwähnten Rédeischen Satz folgendermaßen formulieren ([4], S. 30; [5]):

(2. 1) (RÉDEI) *Richtet man die Kanten eines vollständigen Graphen in beliebiger Weise, so enthält der entstehende gerichtete Graph immer eine Bahn, die den Graphen bedeckt.*[2])

Die Voraussetzung, daß der Graph Γ vollständig ist, kann man auch durch $p_{\max}(\Gamma)=1$ ausdrücken. Diese Formulierung ermöglicht folgende Verallgemeinerung von (2. 1).

(2. 2) Satz. *Gilt für Γ $p_{\max}(\Gamma)=k$ und richtet man die Kanten von Γ in beliebiger Weise, so enthält der entstehende gerichtete Graph immer k oder weniger als k solche Bahnen, die den Graphen bedecken.*

---

[2]) In [5] beweist RÉDEI eine wesentlich tiefere Behauptung. Er zeigt, daß die Anzahl derjenigen Bahnen des in (2. 1) vorkommenden gerichteten Graphen, die in sich allein den Graphen bedecken, ungerade ist.

Wir wollen bemerken: Ist $p_{max}(\Gamma)=k$, so kann man die Kanten von Γ so richten, daß der entstehende Graph $\vec{\Gamma}$ nicht durch weniger, als k Bahnen von $\vec{\Gamma}$ bedeckt werden kann. Um eine solche Richtung der Kanten durchzuführen, wähle man k solche Punkte, die in Γ unabhängig sind und richte sämtliche mit den ausgewählten Punkten inzidente Kanten von Γ in solcher Weise, daß die ausgewählten Punkte die Anfangspunkte dieser Kanten werden.

(2. 2) wollen wir auf den folgenden Satz zurückführen:

(2. 3) Satz. *Ist $\vec{\Gamma}$ azyklisch, so ist die maximale Anzahl der bahnunabhängigen Punkte in $\vec{\Gamma}$ gleich der minimalen Anzahl der bedeckenden Bahnen.*

(Wir bemerken: Die Voraussetzung, daß $\vec{\Gamma}$ azyklisch ist, ist wesentlich.)

Den Satz (2. 3), den wir 1947 gefunden haben[3]), dürfen wir als bewiesen betrachten. Man kann nämlich leicht sehen (diese Ausführungen wollen wir hier unterlassen), daß (2. 3) eine einfache Folge des nachfolgenden Dilworthschen Satzes (2. 4) ist. ([2]. Auch (2. 4) ist eine unmittelbare Folge von (2. 3).)

(2. 4) (Dilworth) *Kann man aus der halbgeordneten endlichen Menge H k paarweise unvergleichbare Elemente auswählen, $k+1$ aber nicht, so kann man H in k paarweise fremde Ketten zerlegen.* (Eine Kette ist eine solche Teilmenge von H, deren Elemente paarweise vergleichbar sind.)[4])

Um (2. 2) auf (2. 3) zurückzuführen, genügt es zu zeigen, daß ein Graph $\vec{\Gamma}$ mit $p_{max}(\vec{\Gamma})=k$ einen solchen azyklischen Teilgraphen $\vec{\Gamma}_1$ besitzt, der jeden Punkt von $\vec{\Gamma}$ enthält und in dem die maximale Anzahl der bahnunabhängigen Punkte nicht größer als k ist. Nehmen wir nun an, daß für $\vec{\Gamma}$ $p_{max}(\vec{\Gamma})=k$ gilt, und bezeichnen wir mit G die Menge derjenigen Teilgraphen von $\vec{\Gamma}$, die azyklisch sind und die jeden Punkt von $\vec{\Gamma}$ enthalten. G ist nicht leer. Derjenige Teilgraph nämlich, der jeden Punkt von $\vec{\Gamma}$ enthält und keine Kante besitzt, ist ein Element von G. Nennen wir nun ein Element $\vec{\Gamma}_i$ von G *maximal*, wenn kein Element von G ein echter Teilgraph von $\vec{\Gamma}_i$ ist. G enthält maximale Elemente. Es sei $\vec{\Gamma}_1$ ein solches Element und $P_1, \ldots, P_h$ seien beliebige, in $\vec{\Gamma}_1$ bahnunabhängige Punkte. Um zu zeigen, daß $\vec{\Gamma}_1$ ein gewünschter Teilgraph von $\vec{\Gamma}$ ist, brauchen wir nur die Ungleichung $h \leqq k$ beweisen. Nehmen wir nun an, daß $h>k$ ist. Dann existiert in $\vec{\Gamma}$ eine Kante, die zwei Punkte der Menge $\{P_1, \ldots, P_h\}$ verbindet. Gehöre z. B. $\overrightarrow{P_1P_2}$ zu $\vec{\Gamma}$.

[3]) Dieser Satz wurde nicht publiziert.

[4]) In [2] beweist Dilworth (2. 4) auch auf unendliche Mengen.

$\overrightarrow{P_1P_2}$ kann nicht in $\vec{\Gamma}_1$ liegen. Fügen wir $\overrightarrow{P_1P_2}$ zu $\vec{\Gamma}_1$, so muß wegen der Maximalität von $\vec{\Gamma}_1$ der entstehende Graph einen Kreis c enthalten. Da $\vec{\Gamma}_1$ azyklisch war, muß c $\overrightarrow{P_1P_2}$ enthalten. Lassen wir nun $\overrightarrow{P_1P_2}$ aus c weg, so bilden die zurückbleibenden Kanten von c eine Bahn von $\vec{\Gamma}_1$, die sowohl P_1 als auch P_2 enthält. Das widerspricht jedoch der Annahme, daß P_1 und P_2 in $\vec{\Gamma}_1$ bahnunabhängig sind.

3. Die im Satz (2. 4) vorkommenden Ketten haben paarweise kein gemeinsames Element. Von den in (2. 3) vorkommenden Bahnen kann man im allgemeinen nicht fordern, daß sie paarweise keinen gemeinsamen Punkt enthalten sollen. Man kann aber diese Forderung bei (2. 2) stellen:

(3. 1) Satz. *Ist für Γ $p_{\max}(\Gamma)=k$ und richtet man die Kanten von Γ in beliebiger Weise, so enthält der entstehende gerichtete Graph $\vec{\Gamma}$ immer k oder weniger als k solche Bahnen, die $\vec{\Gamma}$ bedecken und paarweise keinen gemeinsamen Punkt enthalten.*

Es ist uns nicht gelungen, diesen Satz auf (2. 2) bzw. (2. 3) zurückzuführen. Wir werden jetzt für (3. 1) einen von (2. 2), (2. 3) und (2. 4) unabhängigen Beweis geben. Wir bemerken, daß sich dadurch ein neuer Beweis für (2. 4) (und demzufolge auch für (2. 3)) ergibt. (2. 4) ist nämlich eine einfache Folge von (3. 1). (Auf diese Tatsache hat uns R. RADO aufmerksam gemacht.)

Wir führen einige neue Bezeichnungen ein: Ist $\vec{\Gamma}$ ein beliebiger gerichteter Graph, so soll $\pi(\vec{\Gamma})$ die Anzahl der Punkte von $\vec{\Gamma}$ bezeichnen. Ist S ein Bahnsystem, so bezeichne $\nu(S)$ die Anzahl der Elemente von S und $A(S)$ die Menge der Anfangspunkte der zu S gehörigen Bahnen. Bedeckt ferner das Bahnsystem S den Graphen $\vec{\Gamma}$ und haben je zwei Bahnen von S keinen gemeinsamen Punkt, so wollen wir S ein *zu $\vec{\Gamma}$ passendes* Bahnsystem nennen. Wir legen erst fest:

(3. 2) *Jeder Graph $\vec{\Gamma}$ enthält ein zu $\vec{\Gamma}$ passendes Bahnsystem.*

Ein solches System bekommt man im jedem Falle dadurch, daß man jeden Punkt von $\vec{\Gamma}$ als eine selbständige Bahn betrachtet und die Menge sämtlicher solcher Bahnen bildet.

Wir werden nun (3. 1) dadurch beweisen, daß wir die Richtigkeit des nachfolgenden Satzes (3. 3) zeigen. ((3.2) und (3. 3) sagen gemeinsam etwas mehr aus, als (3.1).)

(3. 3) Satz. *Gilt für $\vec{\Gamma}$ $p_{\max}(\vec{\Gamma})=k$ und ist S ein beliebiges zu $\vec{\Gamma}$ passendes Bahnsystem, so gibt es ein zu $\vec{\Gamma}$ passendes Bahnsystem S^* mit $\nu(S^*)\leqq k$ und $A(S^*)\subseteq A(S)$.*

Beweis. (1) Die Behauptung von (3. 3) ist trivial, falls $\pi(\vec{\Gamma}) = 1$ ist. Nehmen wir an, daß sie für jeden solchen Graphen richtig ist, der weniger als n ($n>1$) Punkte enthält und es bezeichne jetzt $\vec{\Gamma}$ einen Graphen mit $\pi(\vec{\Gamma}) = n$. Wir zeigen, daß unser Satz auch für $\vec{\Gamma}$ gilt. Es sei $p_{\max}(\vec{\Gamma}) = k$ und S ein beliebiges zu $\vec{\Gamma}$ passendes Bahnsystem.

(2) Wir beweisen erst, daß es ein zu $\vec{\Gamma}$ passendes System S' mit $\nu(S') \leqq k+1$ und $A(S') \subseteq A(S)$ gibt. Ist $\nu(S) \leqq k+1$, so kann man $S' = S$ setzen. Ist $\nu(S) > k+1$, so sei b eine beliebige Bahn von S und es bezeichne $\vec{\Gamma}_1$ denjenigen Teilgraphen von $\vec{\Gamma}$, der aus $\vec{\Gamma}$ durch die Weglassung der Punkte von b und der zu diesen Punkten inzidenten Kanten entsteht. Es gilt $\pi(\vec{\Gamma}_1) < n$ und $p_{\max}(\vec{\Gamma}_1) \leqq k$. Das Bahnsystem $S_1 = S - \{b\}$ ist ein zu $\vec{\Gamma}_1$ passendes System. Nach (1) gibt es dann ein zu $\vec{\Gamma}_1$ passendes System S_2 mit $\nu(S_2) \leqq k$ und $A(S_2) \subseteq A(S_1)$. Das System $S' = S_2 \cup \{b\}$ paßt aber zu $\vec{\Gamma}$ und es gilt $\nu(S') \leqq k+1$ und $A(S') \subseteq A(S)$.

(3) Jetzt zeigen wir, daß ein zu $\vec{\Gamma}$ passendes S^* mit $\nu(S^*) \leqq k$ und $A(S^*) \subseteq A(S)$ existiert. Gilt für den unter (2) definierten S' $\nu(S') \leqq k$, so kann man $S^* = S'$ setzen. Nehmen wir nun an, daß $\nu(S') = k+1$ ist. Es sei $S' = \{b_1, \ldots, b_{k+1}\}$ und es bezeichne P_i den Anfangspunkt von b_i ($i = 1, \ldots, k+1$). Da $p_{\max}(\vec{\Gamma}) = k$ ist, gibt es eine Kante von $\vec{\Gamma}$, die zwei Punkte von $A(S') = \{P_1, \ldots, P_{k+1}\}$ verbindet. Es sei z. B. $\overrightarrow{P_1P_2}$ eine Kante von $\vec{\Gamma}$.

Besteht b_1 nur aus dem einzigen Punkt P_1, so füge man $\overrightarrow{P_1P_2}$ zu b_2. Die so entstehende Bahn bildet dann mit den von b_1 verschiedenen Bahnen von S' ein gewünschtes System S^*.

Enthält b_1 außer P_1 noch weitere Punkte, so bezeichne b_1' diejenige Bahn, die aus b_1 durch Weglassung der zu P_1 inzidenten Kante $\overrightarrow{P_1P_1'}$ von b_1 entsteht. (P_1' ist der Anfangspunkt von b_1'.) Es bezeichne ferner $\vec{\Gamma}_2$ denjenigen Teilgraphen von $\vec{\Gamma}$, der aus $\vec{\Gamma}$ durch Weglassung von P_1 und der zu P_1 inzidenten Kanten von $\vec{\Gamma}$ entsteht. Es gilt $\pi(\vec{\Gamma}_2) < n$ und $p_{\max}(\vec{\Gamma}_2) \leqq k$. Es ist weiter $S_3 = \{b_1', b_2, \ldots, b_{k+1}\}$ ein zu $\vec{\Gamma}_2$ passendes System. Nach (1) existiert ein zu $\vec{\Gamma}_2$ passendes $\bar{S} = \{\bar{b}_1, \ldots, \bar{b}_h\}$ mit $h \leqq k$ und $A(\bar{S}) \subseteq A(S_3) = \{P_1', P_2, \ldots, P_{k+1}\}$.

Ist $P_1' \in A(\bar{S})$ und ist z. B. P_1' der Anfangspunkt von $\bar{b}_1$, so füge man $\overrightarrow{P_1P_1'}$ zu $\bar{b}_1$. Die so entstehende Bahn bildet dann mit den von $\bar{b}_1$ verschiedenen Bahnen von $\bar{S}$ ein gesuchtes System S^*.

Ist $P_1' \notin A(\bar{S})$ und $h<k$, so bilden die Bahnen von $\bar{S}$ zusammen mit der Bahn $b^* = (P_1)$ ein gewünschtes S^*.

Ist endlich $P_1' \notin A(\bar{S})$ und $h = k$, so gilt $A(\bar{S}) = \{P_2, \ldots, P_{k+1}\}$. Ist z. B. P_2 der Anfangspunkt von $\bar{b}_1$, so füge man $\overrightarrow{P_1P_2}$ zu $\bar{b}_1$. Die so entstehende Bahn bildet dann mit den von $\bar{b}_1$ verschiedenen Bahnen von $\bar{S}$ ein gewünschtes S^*.

Literaturverzeichnis

[1] G. B. Dantzig and A. J. Hoffman, Dilworth's theorem on partially ordered sets, Linear Inequalities and Related Systems, *Annals of Math. Studies*, **38** (1956), 215—221.

[2] R. P. Dilworth, A decomposition theorem for partially ordered sets, *Annals of Math.*, **51** (1950), 161—166.

[3] T. Gallai, Maximum-Minimum Sätze über Graphen, *Acta Math. Acad. Sci. Hung.*, **9** (1958), 395—434.

[4] D. König, *Theorie der endlichen und unendlichen Graphen* (Leipzig, 1936).

[5] L. Rédei, Ein kombinatorischer Satz, *Acta Sci. Math.*, **7** (1934), 39—43.

[6] T. Szele, Kombinatorikai vizsgálatok az irányított teljes gráffal kapcsolatban, *Math. Fiz. Lapok*, **50** (1943), 223—254.

(Eingegangen am 29. Januar 1960)

СВОБОДНЫЕ СУММЫ МУЛЬТИОПЕРАТОРНЫХ ГРУПП

А. Г. КУРОШ (Москва)

Профессору Л. Редеи к его шестидесятилетию

Введение

Группы с мультиоператорами введены в работе Хиггинса [1]. Именно, группа G, аддитивно записанная, хотя не обязательно коммутативная, называется группой с системой мультиоператоров Ω или, короче, Ω-группой, если всякий оператор $\omega \in \Omega$ является n-арной алгебраической операцией, заданной в G, $n \geqq 1$, причем выполняется требование

$$00\ldots0\omega = 0.$$

К числу Ω-групп принадлежат группы, кольца, а также группы и кольца с операторами. Это понятие весьма хорошо приспособлено, видимо, для того, чтобы служить носителем теорий, объединяющих те параллельные ветви теории групп и теории колец, которые связаны с понятием ядра гомоморфизма и поэтому не могут быть распространены на произвольные универсальные алгебры.

Группы с данной системой мультиоператоров Ω составляют примитивный класс универсальных алгебр. Можно говорить, следовательно, о свободных Ω-группах и ставить, в частности, вопрос об их Ω-подгруппах. Как известно, соответствующий вопрос для свободных групп с операторами (в обычном смысле слова) очень труден: в работе С. Т. Завало [2] описаны допустимые подгруппы свободных групп с группой операторов, причем эти подгруппы уже не обязаны быть свободными.

В случае Ω-групп операторы более сложные, т. е. n-арные, а не только унарные, но зато тождественные соотношения много проще. Оказывается, что в теорию Ω-групп можно перенести не только теорему Нильсена-Шрейера о подгруппах свободных групп, но и теорию свободных разложений. Именно это составляет содержание настоящей работы.

При проведении доказательств мы используем соответствующие результаты из теории групп без операторов, отсылая читателя к гл. 9 книги

автора [3]. Несомненно, что можно было бы дать и независимое изложение теории, т. е. вывести из нее в качестве следствий указанные результаты о свободных группах и свободных произведениях групп без операторов.

Последний параграф работы посвящен рассмотрению аналогичных вопросов для Ω-групп с абелевой аддитивной группой; кольца принадлежат к числу именно таких Ω-групп. Теория идет здесь не так далеко, как в общем случае, так как для прямых разложений абелевых групп не существует столь исчерпывающей теории, как для свободных разложений некоммутативных групп.

§ 1.

Рассматриваем систему мультиоператоров Ω, которая на протяжении всей работы будет считаться фиксированной. Запись $a_1 a_2 \dots a_n \omega$ будет всегда означать, что ω — некоторый n-арный оператор из Ω.

Группа G, аддитивно записанная, будет называться частичной Ω-группой, если в ней уже определены элементы $a_1 a_2 \dots a_n \omega$ для некоторых упорядоченных систем элементов $a_1, a_2, \dots, a_n$ и некоторых операторов $\omega \in \Omega$. При этом предполагается, что для всякого n-арного оператора $\omega \in \Omega$ элемент $00\dots0\omega$ уже определен; причем

$$00\dots0\omega = 0. \tag{1}$$

Всякая группа без мультиоператоров может рассматриваться как частичная Ω-группа, если для всех $\omega \in \Omega$ положить справедливость равенства (1).

Если дана Ω-группа G, то подгруппа U группы G будет в общем случае лишь частичной Ω-группой. Если же U само является Ω-группой, т. е. замкнуто относительно всех операторов из Ω, то оно будет называться Ω-подгруппой Ω-группы G. Ясно, что пересечение любой системы Ω-подгрупп само будет Ω-подгруппой, а поэтому можно говорить об Ω-подгруппе, порожденной данным множеством элементов. С другой стороны, подгруппа U Ω-группы G будет называться чистой подгруппой, если элемент $a_1 a_2 \dots a_n \omega$, где $a_1, a_2, \dots, a_n \in U$, принадлежит к U лишь в том случае, когда $a_1 = a_2 = \dots = a_n = 0$.

Пусть дана частичная Ω-группа G_0. Ω-группа G будет называться ее свободным Ω-замыканием, если 1. $G \supseteq G_0$ и Ω-подгруппа, порожденная в Ω-группе G множеством G_0, совпадает с G; 2. группа G является свободной суммой группы G_0 и свободной группы, систему свободных образующих которой составляют всевозможные элементы вида $a_1 a_2 \dots a_n \omega$, где $a_1, a_2, \dots, a_n \in G$, кроме таких элементов этого вида, что все $a_1, a_2, \dots, a_n \in G_0$ и элемент $a_1 a_2 \dots a_n \omega$ был уже в G_0 определен.

Теорема 1. Для всякой частичной Ω-группы G_0 свободное Ω-замыкание существует и с точностью до Ω-изоморфизма, тождественного на G_0, определено однозначно.

Введем сперва одно обозначение. Если H — произвольная частичная Ω-группа, то через H' будем обозначать частичную Ω-группу, строящуюся следующим образом: группа H' является свободной суммой группы H и свободной группы, имеющей системой свободных образующих множество всевозможных таких символов $a_1a_2 \dots a_n\omega$, где $a_1, a_2, \dots, a_n \in H$, $\omega \in \Omega$, которые в самой частичной Ω-группе H еще не определены; элементы $a_1a_2 \dots a_n\omega$ определены в H' естественным образом тогда и только тогда, когда все $a_1, a_2, \dots, a_n \in H$.

Приступим теперь к доказательству теоремы. Рассмотрим возрастающую последовательность частичных Ω-групп

$$G_0 \subset G_1 \subset \cdots \subset G_n \subset \dots, \tag{2}$$

где

$$G_n = G'_{n-1}, \quad n = 1, 2, \dots. \tag{3}$$

Ясно, что объединение G этой последовательности будет Ω-группой и служит искомым свободным Ω-замыканием для G_0.

Пусть, с другой стороны, $\overline{G}$ будет произвольное свободное Ω-замыкание для G_0. Положим $\overline{G}_0 = G_0$ и φ_0 — тождественное отображение $\overline{G}_0$ на G_0. Пусть в $\overline{G}$ уже выбраны частичные Ω-подгруппы $\overline{G}_i$ для $i = 0, 1, \dots, n-1$, причем $\overline{G}_i \subset \overline{G}_j$ при $i < j$, и установлены продолжающие друг друга Ω-изоморфизмы $\varphi_i: \overline{G}_i \longleftrightarrow G_i$, где G_i из (2). Тогда через $\overline{G}_n$ обозначим подгруппу группы $\overline{G}$, порождаемую подгруппой $\overline{G}_{n-1}$ и всеми теми элементами вида $a_1a_2 \dots a_n\omega$, где $a_1, a_2, \dots, a_n \in \overline{G}_{n-1}$, которые не содержатся в $\overline{G}_{n-1}$. Из определения свободного Ω-замыкания и (3) следует, что существует Ω-изоморфное отображение $\varphi_n: \overline{G}_n \longleftrightarrow G_n$, продолжающее отображение φ_{n-1}. Так как $\overline{G}$ является объединением возрастающей последовательности

$$\overline{G}_0 \subset \overline{G}_1 \subset \cdots \subset \overline{G}_n \subset \dots,$$

то теорема доказана.

§ 2.

Теорема 2. Если Ω-группа G является свободным Ω-замыканием частичной Ω-группы G_0, то всякая Ω-подгруппа U Ω-группы G будет свободным Ω-замыканием подгруппы U', являющейся свободной суммой пересечения $U_0 = U \cap G_0$, не-

которых пересечений вида $U \cap (-g + G_0 + g)$, $g \in G$ (причем для всякого ненулевого пересечения этого вида сопряженная с ним в U подгруппа входит в рассматриваемое свободное разложение для U'), и, наконец, некоторой свободной группы. Подгруппа U' является при этом такой частичной Ω-группой, что элемент $a_1 a_2 \dots a_n \omega$ определен в ней лишь в том случае, если $a_1, a_2, \dots, a_n \in U_0$ и указанный элемент уже был определен в G_0.

В силу определения свободного Ω-замыкания группа G является свободной суммой группы G_0 и бесконечных циклических групп с образующими $a_1 a_2 \dots a_n \omega$, где $a_1, a_2, \dots, a_n \in G$, кроме тех, что $a_1, a_2, \dots, a_n \in G_0$ и элемент $a_1 a_2 \dots a_n \omega$ уже был в G_0 определен. На основании теоремы о подгруппах свободной суммы (свободного произведения) групп для подгруппы U существует разложение в свободную сумму некоторых пересечений вида $U \cap (-g + G_0 + g)$, $g \in G$ (причем войдет, в частности, и пересечение $U_0 = U \cap G_0$ и имеет место утверждение, высказанное в формулировке теоремы в скобках), и некоторых бесконечных циклических подгрупп. Среди них войдут, как входящие в исходное свободное разложение для G, все бесконечные циклические подгруппы, порожденные элементами $a_1 a_2 \dots a_n \omega$, где $a_1, a_2, \dots, a_n \in U$, кроме тех, что $a_1, a_2, \dots, a_n \in U_0$ и элемент $a_1 a_2 \dots a_n \omega$ уже был определен в G_0, т. е. уже содержится в U_0.

Все, кроме этих последних, свободные слагаемые из полученного нами свободного разложения для U порождают подгруппу U', являющуюся их свободной суммой и, как частичная Ω-группа, удовлетворяющую тому, что высказано в формулировке теоремы. Больше того, U будет свободным Ω-замыканием для U', если мы покажем, что Ω-подгруппа $\bar{U}'$, порожденная в Ω-группе G множеством U', совпадает с U.

Для доказательства построим в G последовательность подгрупп (2) со свойством (3). Пусть уже доказано, что пересечение $U_n = U \cap G_n$ содержится в $\bar{U}'$ — для $n = 0$ это очевидно. Если $a_1, a_2, \dots, a_n \in U$ и $a_1 a_2 \dots a_n \omega \in U_{n+1}$, то $a_1, a_2, \dots, a_n \in U_n \subset \bar{U}'$, а поэтому и элемент $a_1 a_2 \dots a_n \omega$ содержится в Ω-подгруппе $\bar{U}'$. Следовательно $U_{n+1} \subset \bar{U}'$, т. е. $\bar{U}' = U$. Теорема доказана.

§ 3.

Возьмем свободную группу F_0 с системой свободных образующих N и положим, что для всех операторов ω из заданной системы мультиоператоров Ω в F_0 выполняются равенства (1). Свободное Ω-замыкание F группы F_0 будет называться свободной Ω-группой, а множество

N — ее системой свободных образующих. Подгруппа F_0 будет, следовательно, чистой в F.

Ясно, что свободные Ω-группы действительно являются свободными в классе всех Ω-групп, рассматриваемом как примитивный класс универсальных алгебр: всякое отображение множества N в произвольную Ω-группу H можно продолжить, притом единственным способом, до Ω-гомоморфизма F в H.

Теорема 3. Мощность системы свободных образующих является инвариантом свободной Ω-группы.

Действительно, пусть в свободной Ω-группе F выбраны две системы свободных образующих, N и N'. Положим

$$\{N\} = F_0, \quad \{N'\} = F_0'.$$

Эти обе подгруппы являются чистыми, а поэтому группа F представляется в виде свободной суммы *любой* из них и одной и той же третьей подгруппы, а именно свободной подгруппы, имеющей системой свободных образующих множество всевозможных элементов вида $a_1 a_2 \dots a_n \omega$ для любых $\omega \in \Omega$ и любых элементов $a_1, a_2, \dots, a_n \in F$, которые не все равны нулю. Отсюда следует, что свободные группы F_0 и F_0' изоморфны между собой.

Теорема 4. Всякая Ω-подгруппа U свободной Ω-группы F сама является свободной Ω-группой.

Действительно, по теореме 2 U будет свободным Ω-замыканием подгруппы U', которая будет в нашем случае чистой и, ввиду теоремы о подгруппах свободных групп, свободной.

Теорема доказана. Очевидно, что если система мультиоператоров Ω не является пустой, то в свободной Ω-группе с одним образующим можно найти свободные Ω-подгруппы с бесконечным множеством свободных образующих.

§ 4.

Если дано семейство Ω-групп H_i, $i \in I$, то свободная сумма G_0 этих групп,

$$G_0 = \sum_{i \in I}^{*} H_i,$$

будет частичной Ω-группой: элемент $a_1 a_2 \dots a_n \omega$ определен в ней тогда и только тогда, если все элементы $a_1, a_2, \dots, a_n$ принадлежат к одной и той же подгруппе H_i. Свободное Ω-замыкание G этой частичной Ω-группы мы

будем называть свободной Ω-суммой заданных Ω-групп H_i, $i \in I$, и записывать в виде

$$G = \sum_{i \in I}^{*}{}_{\Omega} H_i$$

или, в случае конечного числа свободных слагаемых, в виде

$$G = H_1 *_{\Omega} \cdots *_{\Omega} H_n.$$

Из этого определения немедленно вытекают следующие свойства:

1. Пусть Ω-группа G является свободным Ω-замыканием частичной Ω-группы G_0 и пусть

$$G_0 = \sum_{i \in I}^{*} H_i.$$

Предположим, что если элемент $a_1 a_2 \dots a_n \omega$ определен в G_0, то все элементы $a_1, a_2, \dots, a_n$ содержатся в одной и той же подгруппе H_i и сам элемент $a_1 a_2 \dots a_n \omega$ принадлежит к этой же подгруппе H_i. Тогда Ω-группа G будет свободной Ω-суммой свободных Ω-замыканий частичных Ω-подгрупп H_i, $i \in I$.

Отсюда следует

2. Свободная Ω-группа F с системой свободных образующих N является свободной Ω-суммой свободных Ω-групп с одним образующим, а именно порожденных всеми элементами из N.

3. Если

$$G = \sum_{i \in I}^{*}{}_{\Omega} A_i \tag{4}$$

и если

$$A_i = \sum_{j \in J_i}^{*}{}_{\Omega} B_{ij}, \quad i \in I,$$

то

$$G = \sum_{i \in I,\, j \in J_i}^{*}{}_{\Omega} B_{ij}. \tag{5}$$

Разложение (5) будет называться продолжением разложения (4).

4. Если

$$G = \sum_{i \in I}^{*}{}_{\Omega} A_i$$

и если множество индексов I представлено как объединение непересекающихся подмножеств I_s, $s \in S$, то

$$G = \sum_{s \in S}^{*}{}_{\Omega} B_s,$$

где

$$B_s = \sum_{i \in I_s}^{*}{}_{\Omega} A_i.$$

5. Если

$$G=\sum_{i\in I}^{*}{}_{\Omega} A_i$$

и если заданы Ω-гомоморфизмы φ_i Ω-групп A_i в некоторую Ω-группу H, то существует, притом единственный, Ω-гомоморфизм $\varphi: G \to H$, совпадающий на A_i с φ_i, $i \in I$.

§ 5.

Теорема 5. Всякая Ω-подгруппа U свободной Ω-суммы Ω-групп H_i, $i \in I$, является свободной Ω-суммой ненулевых пересечений $U \cap H_i$, $i \in I$, свободных Ω-замыканий некоторых своих чистых подгрупп вида $U \cap (-g + H_i + g)$, $g \in G$, $i \in I$ (причем для всякого ненулевого пересечения такого вида свободное Ω-замыкание подгруппы, сопряженной с ним в U, входит в рассматриваемое свободное разложение для U) и, наконец, некоторой свободной Ω-группы.

В самом деле, пусть

$$G=\sum_{i\in I}^{*}{}_{\Omega} H_i$$

и пусть

$$G_0=\sum_{i\in I}^{*} H_i.$$

По теореме 2 подгруппа U будет свободным Ω-замыканием подгруппы U', являющейся свободной суммой пересечения $U \cap G_0$, некоторых подгрупп вида $U \cap (-g + G_0 + g)$, $g \in G$, и свободной подгруппы. По теореме о подгруппах свободной суммы пересечение $U \cap G_0$ является свободной суммой ненулевых пересечений $U \cap H_i$, $i \in I$, некоторых подгрупп вида $U \cap (-g_0 + H_i + g_0)$, $g_0 \in G_0$, и некоторой свободной группы. Аналогичные свободные разложения существуют и для подгрупп $U \cap (-g + G_0 + g)$.

Мы получаем новое свободное разложение для U', причем, в силу теоремы 2 и определения G_0 как частичной Ω-группы, U' будет такой частичной Ω-группой, что элемент $a_1 a_2 \dots a_n \omega$ определен в ней тогда и только тогда, если все элементы $a_1, a_2, \dots, a_n$ принадлежат к одному и тому же пересечению $U \cap H_i$, причем элемент $a_1 a_2 \dots a_n \omega$ принадлежит тогда к этому же пересечению. Отсюда, ввиду свойства 1, следует основное утверждение теоремы. Что же касается утверждения, высказанного в скобках, то оно вытекает из справедливости соответствующего утверждения в теореме 2 и в теореме о подгруппах свободной суммы групп без мультиоператоров.

§ 6.

Напомним, что идеал A Ω-группы G есть такой нормальный делитель группы G, что для любых $\omega \in \Omega$, $a_1, a_2, \ldots, a_n \in A$ и $b_1, b_2, \ldots, b_n \in G$ имеет место включение

$$(a_1 + b_1)(a_2 + b_2) \cdots (a_n + b_n)\omega \in b_1 b_2 \ldots b_n \omega + A. \tag{6}$$

Отметим еще одно свойство свободных Ω сумм:

6. Если $G = A \overset{*}{\underset{\Omega}{+}} B$, то Ω-группа B Ω-изоморфна Ω-факторгруппе G по идеалу $\bar{A}$, порожденному A.

Для доказательства построим в G, как в свободном Ω-замыкании частичной Ω-группы $G_0 = A * B$, последовательность (2). Пусть уже доказано, что всякий элемент из G_k лежит в одном смежном классе по $\bar{A}$ с некоторым элементом из B — для $k = 0$ это очевидно. Для того, чтобы доказать это утверждение для $k+1$, достаточно показать это для элемента вида $x_1 x_2 \ldots x_n \omega$, где $x_i \in G_k$, $i = 1, 2, \ldots, n$. Однако, по индуктивному предположению

$$x_i = \bar{a}_i + \bar{b}_i, \quad \bar{a}_i \in \bar{A}, \quad b_i \in B, \quad i = 1, 2, \ldots, n,$$

после чего остается воспользоваться включением (6). С другой стороны, $\bar{A} \cap B = 0$ ввиду 5.

Теорема 6. Если даны два свободных Ω-разложения Ω-группы G,

$$G = \sum_{i \in I}^{*}{}_{\Omega} A_i = \sum_{j \in J}^{*}{}_{\Omega} B_j, \tag{7}$$

то для них можно построить такие продолжения, слагаемые которых взаимно однозначно соответствуют друг другу, причем соответствующие слагаемые или совпадают — они имеют тогда вид $A_i \cap B_j$, — или являются свободными Ω-замыканиями сопряженных между собою чистых подгрупп, или же, наконец, являются изоморфными свободными Ω-группами.

В самом деле, мы получим искомые продолжения, если разложим на основании теоремы 5 всякое A_i, $i \in I$, относительно второго из разложений (7), всякое B_j, $j \in J$, — относительно первого из этих разложений, а затем разумным образом объединим слагаемые, являющиеся свободными Ω-группами. Всякое ненулевое пересечение $A_i \cap B_j$ войдет при этом свободным слагаемым в каждое из указанных продолжений.

С другой стороны, в первое [второе] продолжение входят также свободные Ω-замыкания некоторых чистых подгрупп вида $A_{i\alpha} = A_i \cap$

$\cap(-g+B_j+g)$ [соответственно вида $B_{j\beta}=B_j\cap(-g'+A_i+g')$]. Однако $B_{j\beta}$ сопряжено с пересечением $A_i\cap(g'+B_j-g')$, но, по теореме 5, в первое из рассматриваемых продолжений входит в качестве свободного слагаемого свободное Ω-замыкание некоторой сопряженной с этим пересечением подгруппы $A_{i\alpha}$. Так как эти рассуждения можно обратить и так как подгруппа $A_{i\alpha}$ не может быть сопряжена ни с какой другой подгруппой этого же вида и ни с каким пересечением вида $A_i\cap B_j$ — они входят свободными слагаемыми в одно и то же свободное разложение группы G, — то мы получаем взаимно однозначное соответствие и между рассматриваемыми свободными слагаемыми второго вида.

Наконец, объединения свободных слагаемых рассмотренных двух видов, взятые в каждом из продолжений, порождают в G один и тот же идеал. Отсюда следует, по свойству 6, что объединения свободных слагаемых из этих продолжений, являющихся свободными Ω-группами, Ω-изоморфны между собой. Теорема доказана.

§ 7.

Ω-группа G с абелевой аддитивной группой будет называться ΩA-группой. Аналогично определяется частичная ΩA-группа.

ΩA-группа G будет называться свободным ΩA-замыканием частичной ΩA-группы G_0, если 1. $G\supseteq G_0$ и Ω-подгруппа, порожденная в G множеством G_0, совпадает с G; 2. группа G является прямой суммой группы G_0 и свободной абелевой группы, базу которой составляют всевозможные элементы вида $a_1a_2\ldots a_n\omega$, где $a_1, a_2, \ldots, a_n\in G$, кроме таких, что все $a_1, a_2, \ldots, a_n\in G_0$ и элемент $a_1a_2\ldots a_n\omega$ был уже в G_0 определен.

Как и в § 1, доказывается

Теорема 1′. Для всякой частичной ΩA-группы G_0 свободное ΩA-замыкание существует и с точностью до Ω-изоморфизма, тождественного на G_0, определено однозначно.

Теорема 2′. Если ΩA-группа G является свободным ΩA-замыканием частичной ΩA-группы G_0, то всякая Ω-подгруппа U ΩA-группы G будет свободным ΩA-замыканием прямой суммы пересечения $U\cap G_0$ и некоторой свободной абелевой подгруппы.

Доказательство проходит по тому же плану, как и в § 2, но используется, понятно, не теорема о подгруппах свободного произведения, а следующее утверждение, доказываемое по существу так же, как теорема о подгруппах свободной абелевой группы в книге [3]:

Если абелева группа G является прямой суммой абелевой группы G_0 и свободной абелевой группы с базой M, то всякая подгруппа U группы G является прямой суммой пересечения $U \cap G_0$ и некоторой свободной абелевой группы, к базе которой принадлежит, в частности, всякий элемент из M, содержащийся в U.

Свободное ΩA-замыкание F свободной абелевой группы F_0 с базой N, причем для всех $\omega \in \Omega$ в F_0 выполняются равенства (1), называется свободной ΩA-группой, а множество N — ее системой свободных образующих.

Как и в § 3, доказываются теоремы:

Теорема 3′. Мощность системы свободных образующих является инвариантом свободной ΩA-группы.

Теорема 4′. Всякая Ω-подгруппа свободной ΩA-группы сама является свободной ΩA-группой.

Остается справедливым и замечание, что если система мультиоператоров Ω не является пустой, то в свободной ΩA-группе с одним образующим можно найти свободные ΩA-подгруппы с бесконечным множеством свободных образующих.

Литература

[1] P. J. Higgins, Groups with multiple operators, *Proc. London Math. Soc.*, **6** (1956), 366—416.

[2] С. Т. Завало, Операторные Γ-свободные группы, Мат. сборник, **33** (1953), 399—432.

3] А. Г. Курош, Теория групп, 2-е изд. (Москва, 1953).

(Поступило 31/I 1960 г.)

On linked products of groups

By B. H. NEUMANN and HANNA NEUMANN in Sale (Cheshire, England)

To Ladislaus Rédei for his 60th birthday

1. Introduction

Linked products were first introduced in a recent paper [5] by JAMES WIEGOLD and the second author; a number of questions were left unanswered there. We propose to answer some of them in this note.

The products considered are generalizations of GOLOVIN's regular products: the group G is a regular product of its subgroups A and B, if A and B generate G and are retracts (that is, images under idempotent endomorphisms) of G; or, equivalently, the normal closure of A in G meets B trivially, and the normal closure of B in G meets A trivially. In the case of a linked product we ask for a group G generated by A and B in such a way that, although A and B have still only the unit element in common in G, mapping A onto the trivial group induces a prescribed homomorphism of B onto a factor group B/Y, and mapping B onto the trivial group induces a prescribed homomorphism of A onto A/X; in other words, we call G a *linked product of A and B with kernels X and Y* if G is generated by A and B, if A and B have only the unit element in common, but the normal closure of A in G meets B in Y, and the normal closure of B in G meets A in X. We think of A and its normal subgroup X, and of B and its normal subgroup Y, as given.

The question immediately arises whether it is always possible to construct a linked product of given groups A and B with given kernels X and Y. It was shown in [5], Example 6.2, that this is certainly not possible when A and B are both of order 2, and of the kernels X and Y one is trivial and the other not. But the positive results obtained in [5] strongly suggested that this case is, in fact, the only exception. We still can not prove this conjecture, but we make somme further progress towards it. The "unsymmetrical case", where just one of the kernels is trivial, proved the more resistant case in [5]. One of our results here reduces it in many cases — we conjecture:

in all but one case — to the "symmetrical case", where both kernels are non-trivial (§3). (We are not concerned with the case that both kernels are trivial: this is, of course, just the case of GOLOVIN's regular products.) Using results of [5] based on a theorem of WIELANDT [6], we establish in particular the existence of linked products of arbitrary finite groups A and B with arbitrarily prescribed normal subgroups X and Y as kernels, apart, of course, from the one exceptional case described above. Moreover the proof of the reduction theorem shows that these linked products of finite groups can be chosen finite. This confirms another conjecture made in [5].

It is fairly obvious that linked products, where they exist, are not uniquely determined by their constituents A and B and the kernels X and Y. In §5 we give some indication just how widely they may differ: If A and B are finite and X and Y non-trivial proper normal subgroups of A and B, we show — subject to some restrictions on the orders and indices of X and Y arising out of the exceptional case — that there exist finite linked products of A and B in which the kernels X and Y generate a simple group, but there also are finite linked products of A and B in which X and Y generate their direct product.

In §4 we prepare the ground for these constructions by restating some known facts on the embedding of group amalgams.

2. Notation

Groups are denoted by capital letters, their elements by small letters. We write a^b for $b^{-1}ab$, and $[a, b]$ for the commutator $a^{-1}b^{-1}ab$. The unit element of all groups is denoted by 1; the trivial group is always denoted by E. Small Greek letters stand for homomorphisms of groups. Capital German letters are used for group amalgams, that is for set-theoretical unions of given groups intersecting pairwise in given subgroups, with multiplication defined — in the natural way — for those and only those pairs of elements that belong to one and the same constituent group of the amalgam.

If the group G is generated by the set M, we write $G = \mathrm{gp}(M)$; similarly $G = \mathrm{gp}(A, B)$ means that G is generated by its subgroups A, B. If $G = \mathrm{gp}(A, B)$, then the group generated by all commutators $[a, b]$, $a \in A$, $b \in B$, is normal in G (cf. GOLOVIN [1]). It is denoted by $[A, B]$ and called the *cartesian subgroup* of G. If $G = \mathrm{gp}(A, B) = [A, B]$, we call G *self-cartesian*.

The normal closure in G of a set M, that is the least normal subgroup of G containing M, is denoted by M^G. If again $G = \mathrm{gp}(A, B)$, then the normal closure of A in G is $A^G = A \cdot [A, B]$ (cf. GOLOVIN [1]).

Finally we denote the order of a group G by $|G|$.

3. A reduction theorem

In [5], certain reduction theorems were obtained which deduced the existence of a linked product of A and B with kernels X and Y from that of a linked product of X and Y with kernels X and Y — if both X and Y are non-trivial — or from a linked product of X and B with kernels X and E in the unsymmetrical case. Here we prove a reduction theorem which operates, as it were, in the opposite direction: it deduces the existence of a linked product of A and B with kernels X and Y from that of certain linked products of A and B with kernels A and B:

Theorem 3.1. *Let there be a self-cartesian linked product G of A and B with kernels A and B, and let X and Y be arbitrary normal subgroups of A and B, respectively. Then there exists a linked product of A and B with kernels X and Y.*

Proof. Let φ be the canonic epimorphism of A onto $A_1 = A/X$, and ψ the canonic epimorphism of B onto $B_1 = B/Y$. We form the direct product

$$G_0 = A_1 \times G \times B_1;$$

its elements are the triplets $(a\varphi, g, b\psi)$ where a, g, b range over A, G, B, respectively. The triplets

$$a_0 = (a\varphi, a, 1)$$

form a group A_0 which is clearly isomorphic to A; the subgroup X_0 of A_0 corresponding to X consists of the triples $x_0 = (1, x, 1)$. Similarly, the triplets

$$b_0 = (1, b, b\psi)$$

form a group B_0 isomorphic to B, and the triplets $y_0 = (1, y, 1)$ form the subgroup Y_0 of B_0 that corresponds to Y in B.

We prove that G_0 is a linked product of A_0 and B_0 with kernels X_0 and Y_0. Firstly, any element of G_0 common to A_0 and B_0 has first and third components 1, and as $A \cap B = E$, also middle component 1; hence in G_0,

$$A_0 \cap B_0 = E.$$

Secondly, we find the cartesian subgroup $[A_0, B_0]$ of $\mathrm{gp}(A_0, B_0)$. A typical commutator $[a_0, b_0]$ is of the form

$$[a_0, b_0] = (1, [a, b], 1),$$

and as the commutators $[a, b]$ are assumed to generate G, the commutators $[a_0, b_0]$ generate $E \times G \times E$. We identify this subgroup of G_0 with G and then have

$$[A_0, B_0] = G.$$

But A_0 and G generate A_1 (similarly identified with $A_1 \times E \times E \leqq G_0$), and B_0 and G generate B_1; thus A_0 and B_0 between them generate all three direct factors of G_0, and

$$G_0 = \mathrm{gp}(A_0, B_0).$$

Finally

$$A_0^{G_0} = A_0[A_0, B_0] = A_0 G = A_1 \times G.$$

Thus $A_0^{G_0} \cap B_0 = (A_1 \times G) \cap B_0$, and this consists of all elements $(a\varphi, g, 1)$ that are simultaneously of the form $(1, b, b\psi)$. It follows that $a\varphi = 1, g = b$, and $b\psi = 1$; hence $b = y \in Y$, and the elements of the intersection are just the elements

$$y_0 = (1, y, 1).$$

Thus

$$A_0^{G_0} \cap B_0 = Y_0.$$

A symmetrical argument shows that

$$A_0 \cap B_0^{G_0} = X_0,$$

and the theorem follows. The following is an immediate consequence of the proof, as G_0 clearly is finite when G is.

Corollary 3.11. *If G is finite, the linked product also can be taken finite.*

Corollary 3.12. *If the linked product G of A and B with kernels A and B is not only self-cartesian, but simple, then in G_0 — constructed as in the proof of the theorem — every non-trivial subgroup C_0 of A_0 has the property*

$$C_0^{G_0} \cap B_0 = Y_0,$$

and symmetrically, for every $D_0 \leqq B_0, D_0 \neq E$,

$$A_0 \cap D_0^{G_0} = X_0.$$

If both A and B are of order 2, generated by a and b, respectively, then the condition of the theorem cannot be satisfied. For in this case, as $a^2 = b^2 = 1$, the group generated by a and b is dihedral, of order $2n$ or of infinite order; in either case the commutator $[a, b] = (ab)^2$ is an element of the cyclic subgroup of index 2, and therefore cannot generate the whole group. This is, of course, in accordance with the fact that in this case there is no linked product of A and B with kernels A and E.

Again we conjecture that this is the only exception, that is, that any two groups A and B not both of which are of order 2 possess a self-cartesian linked product with kernels A and B. We cannot prove this in general.

If, however, A and B are finite and not both of order 2, then by a theorem of WIELANDT [6] A and B can be so embedded in a finite simple group G, that G is generated by A and B and their intersection in G is trivial; but clearly a simple group is self-cartesian (with respect to any two non-trivial subgroups that generate it). Thus we have:

Theorem 3.2. *Given two finite groups A and B with normal subgroups X and Y, where $E \leqq X \leqq A$ and $E \leqq Y \leqq B$; then there is a finite linked product of A and B with kernels X and Y, unless $|A| = |B| = |X| \cdot |Y| = 2$.*

It may be remarked that here we have the situation in which Corollary 3.12 applies.

Here X and Y will not in general themselves generate a simple group. In order to establish the existence of linked products with this additional property, we have to go back to the procedure used in [5], §3, of building up the linked product of A and B from a linked product of the kernels X and Y. In order to ensure that these linked products also are finite when A and B are finite, we need some facts on embeddings of amalgams of groups.

4. Two lemmas

Let $\mathfrak{A}$ be an amalgam of finitely many finite groups. We assume that $\mathfrak{A}$ is embeddable in a group; therefore the generalized free product F of $\mathfrak{A}$ exists. F is characterized by the facts that it embeds the amalgam $\mathfrak{A}$, is generated by it, and that every homomorphism of $\mathfrak{A}$ into a group can be continued to a homomorphism of F into that group. We further assume[1]) that $\mathfrak{A}$ can be embedded in a finite group P, say, which we may assume to be generated by $\mathfrak{A}$.

Lemma 4.1. [3] *If φ is a homomorphism of $\mathfrak{A}$ into a finite group D, then there is an embedding θ of $\mathfrak{A}$ in a finite group Q generated by $\mathfrak{A}\theta$ and a homomorphism ψ of Q into D such that*

$$\varphi = \theta\psi.$$

For the sake of completeness we here briefly indicate the proof (cf. [3], § 2, where the lemma is proved in a slightly more general situation).

Let $D_1 = \mathrm{gp}(\mathfrak{A}\varphi)$. Then $D_1 \cong F/M$, where F is the generalized free product of $\mathfrak{A}$ and M a normal subgroup of finite index in F. Similarly $P \cong F/N$ where N also has finite index in F. Then $M \cap N$ also is a normal

[1]) It is not known whether this is really an additional assumption, or whether a finite amalgam that is embeddable in a group is also embeddable in a finite group; cf. [2], § 5.

subgroup of finite index in F, and we put $Q = F/M \cap N$. The canonic epimorphism F onto Q induces a homomorphism θ of $\mathfrak{A}$ into Q, and this is a monomorphism because it can be further multiplied by an epimorphism of Q onto P so as to result in the given embedding of $\mathfrak{A}$ in P. We take as ψ the canonic homomorphism of Q onto its factor group $Q/(M/M \cap N) \cong F/M \cong D_1$ followed by an isomorphism onto D_1.

The amalgams to which we are going to apply this lemma are sufficiently simple that we can easily check the validity of the embeddability assumptions made for Lemma 4.1. We use the following known fact ([4], Corollary 15.2).

Lemma 4.2. *An amalgam of two finite groups is embeddable in a finite group.*

5. Some special types of linked product

Let A and B be groups containing the non-trivial normal subgroups X and Y, respectively. Let Z be a linked product of X and Y with kernels X and Y. We form the amalgam $\mathfrak{A}$ of the groups A, B, and Z amalgamating E between A and B, X between A and Z, and Y between B and Z. It is fairly easily seen (and shown in detail in [5], § 3) that the free product of A, B, Z with these amalgamations exists and is a linked product of A and B with kernels X and Y.

If X and Y are finite, we know that such a linked product Z of X and Y with kernels X and Y exists and can be taken finite; and that, moreover, it can be taken as a simple group unless both X and Y have order 2 (WIELANDT [6]). But even if A and B are also finite, the free product will be an infinite group as at least one of A and B contains X, or Y, properly. To construct a finite linked product also in this case, we use Lemma 4.1.

It was stated already that the amalgam $\mathfrak{A}$ of A, B, and Z is embeddable in a group. To see that it is embeddable in a finite group, we first note that, by Lemma 4.2, the subamalgam formed by A and Z amalgamating X is embeddable in a finite group, A_1, say. Similarly the subamalgam formed by B and Z is embeddable in a finite group, B_1, say. We consider the amalgam $\mathfrak{B}$ of A_1 and B_1 amalgamating Z. It contains $\mathfrak{A}$ as a subamalgam. But, again by Lemma 4.2, $\mathfrak{B}$ is embeddable in a finite group, and so, therefore, is $\mathfrak{A}$. Finally, $\mathfrak{A}$ possesses a homomorphism φ into the direct product $D = A/X \times B/Y$; for mapping $A \to A/X$ and $B \to B/Y$ canonically induces automatically the mapping of Z on E. The assumptions of Lemma 4.1 are therefore satisfied, and we deduce:

Lemma 5.1. *The amalgam $\mathfrak{A}$ of A, B, and Z can be embedded in a finite group Q generated by it, such that there exists a homomorphism ψ of Q onto $D = A/X \times B/Y$ which maps A in Q onto $A\psi = A/X$ and B in Q onto $B\psi = B/Y$, canonically.*

We now show that this group Q is a linked product of A and B with kernels X and Y. Q is clearly generated by A and B, as it is generated by $\mathfrak{A}$, and the constituent Z of $\mathfrak{A}$ is generated by $X \leqq A$ and $Y \leqq B$. Also $A \cap B = E$ in $\mathfrak{A}$, and therefore in Q. Finally $A^{\varphi} \geqq X^{\varphi} \geqq Y$, and therefore $A^{\varphi} \cap B \geqq Y$. To show that this intersection cannot contain Y properly, it suffices to exhibit one normal subgroup K of Q which contains A and meets B exactly in Y. Now Q possesses a homomorphism ψ onto $D = A/X \times B/Y$; and D can be mapped homomorphically onto B/Y by the retraction that maps A/X onto E. The product of these homomorphisms is a homomorphism β of Q onto B/Y which maps A onto E and B onto B/Y canonically. The kernel K of β contains A and intersects B in Y, as required. Similarly one shows that $B^{\varphi} \cap A = X$, which completes the argument. We have therefore:

Theorem 5.2. *If A and B are finite groups, if X and Y are non-trivial normal subgroups of A and B, respectively, and if not both of X and Y have order 2, then there exists a finite linked product of A and B, with kernels X and Y, in which X and Y generate a simple group.*

In order to obtain the other extreme, a linked product in which X and Y centralize each other, we first use the methods of § 3 to prove:

Lemma 5.3. *If A/X and Y are finite, non-trivial groups and not both of order 2, then there exists a linked product of A and Y with kernels E and Y in which X and Y centralize each other.*

Proof. Let φ be the canonic epimorphism of A onto $A\varphi = A/X$. As $A\varphi$ and Y do not both have order 2, there exists a self-cartesian linked product G of $A\varphi$ and Y with kernels $A\varphi$ and Y. We form the direct product

$$H_1 = A \times G,$$

and consider in it the group A_0 consisting of all elements $a_0 = (a, a\varphi)$. Again A_0 is isomorphic to A, and we show that H_1 is a linked product of A_0 and Y of the required kind; here Y is thought of as identified with the group consisting of all $y_0 = (1, y)$.

As $[a_0, y] = [(a, a\varphi), (1, y)] = (1, [a\varphi, y])$, and as $[A\varphi, Y] = G$, we have (upon identifying $E \times G \leqq H_1$ with G)

$$[A_0, Y] = G.$$

But A_0 and G generate $A \times E$, and therefore H_1, so that $H_1 = \mathrm{gp}(A_0, Y)$.

Further $A_0^{H_1} = A_0 \cdot [A_0, Y] = A_0 \cdot G = H_1 \geqq Y$, but

$$Y^{H_1} = (Y^G)^{H_1} = G^{H_1} = G,$$

and so $Y^{H_1} \cap A_0$ consists of those elements $(a, a\varphi)$ for which $a = 1$, that is, $Y^{H_1} \cap A_0 = E$. Thus H_1 is a linked product of A_0 and Y with kernels E and Y; and if the subgroup X_0 of A_0 consisting of all elements $(x, 1)$ is identified with X in A, it is clear that together with Y in G it generates the direct product $X \times Y$.

The lemma puts us in a position to construct the kind of linked product we want:

Theorem 5.4. *If A and B are finite groups with non-trivial proper normal subgroups X and Y, respectively, and if neither A/X and Y, nor B/Y and X are simultaneously of order 2, then there exists a finite linked product of A and B, with kernels X and Y, in which X and Y centralize each other.*

Proof. Construct, by Lemma 5.3, a linked product H_1 of A and Y, with kernels E and Y, in which X and Y centralize each other. Symmetrically, also by Lemma 5.3, construct a linked product H_2 of X and B, with kernels X and E, in which X and Y also centralize each other.

The subgroup generated by X and Y is their direct product in both H_1 and H_2, and we denote it by the same letter, T, say, in both. Let $\mathfrak{A}$ be the amalgam of H_1 and H_2 amalgamating T. Then $\mathfrak{A}$ possesses a finite embedding, by Lemma 4.2. Also, by mapping Y onto E and A identically, H_1 is mapped homomorphically onto A. By further mapping A canonically onto A/X we obtain, therefore, a homomorphism φ_1 of H_1 onto A/X in which A is mapped canonically. Similarly there is a homomorphism φ_2 of H_2 onto B/Y which maps B canonically. The two homomorphisms φ_1 and φ_2 agree on $T = X \times Y$, which is mapped on E by both. If, therefore, we define the mapping φ of $\mathfrak{A}$ into $D = A/X \times B/Y$ by $\varphi = \varphi_1$ on H_1 and $\varphi = \varphi_2$ on H_2, then φ maps the amalgam $\mathfrak{A}$ homomorphically into D. By Lemma 4.1, there exists a finite group Q embedding the amalgam $\mathfrak{A}$ and generated by it, such that Q possesses a homomorphism ψ mapping it onto D in such a way that A and B are mapped as by φ, that is canonically onto A/X and B/Y, respectively.

Again we can show now that Q is a linked product of A and B with kernels X and Y; for Q is generated by H_1 and H_2, that is by A, Y, B, and X, and thus by A and B. Also

$$A \cap B \leqq H_1 \cap H_2 = T = X \times Y,$$

and so $A \cap B = (A \cap T) \cap (B \cap T) = X \cap Y = E$.

Finally $A^Q \geqq A^{H_1} \geqq Y$, and so $A^Q \cap B \geqq Y$. But, as before, Q possesses a homomorphism ψ onto $A/X \cap B/Y$, and therefore also a homomorphism β mapping A on E and B canonically onto B/Y. The kernel of β is a normal subgroup of Q which contains A and intersects B exactly in Y, and so it follows that $A^Q \cap B = Y$. Similarly one shows that $B^Q \cap A = X$. Finally X and Y generate the direct product $T = X \times Y$ in Q, so that Q is a linked product of the required kind, and the theorem follows.

References

[1] O. N. Golovin, Nilpotent products of groups, *Mat. Sbornik*, (N. S.) **27 (69)** (1950), 427—454; *Amer. Math. Soc. Translations* (2nd Ser.), **2** (1956), 89—115.

[2] B. H. Neumann and Hanna Neumann, A contribution to the embedding theory of group amalgams, *Proc. London Math. Soc.*, (3) **3** (1953), 243—256.

[3] B. H. Neumann and Hanna Neumann, Partial endomorphisms of finite groups, *J. London Math. Soc.*, **29**, (1954), 434—440.

[4] B. H. Neumann, An essay on free products of groups with amalgamations, *Phil. Trans. Roy. Soc. London*, (A) **246**, (1954), 503—554.

[5] Hanna Neumann and James Wiegold, Linked products and linked embeddings of groups, *Math. Zeitschr.*, **73** (1960), 1—19.

[6] Helmut Wielandt, Einbettung zweier Gruppen in eine einfache Gruppe, *Math. Zeitschr.*, **73** (1960), 20—21.

THE UNIVERSITY, MANCHESTER,
THE MANCHESTER COLLEGE OF SCIENCE AND TECHNOLOGY

(Received January 31, 1960)

Über die Gruppen $PSL_n(q)$, die eine Untergruppe von Primzahlindex enthalten

Von NOBORU ITÔ in Nagoya (Japan)

Herrn Professor Dr. Ladislaus Rédei zum 60. Geburtstag

Über Permutationsgruppen vom Primzahlgrad hat man schon lange gearbeitet. Doch scheint es uns, daß man bis jetzt noch zu wenig Beispiele davon kennt. Daher dürfte es nicht ohne Interesse sein, aus einigen bekannten Klassen von Gruppen diejenigen Gruppen auszuwählen und zu untersuchen, die sich als Permutationsgruppen von Primzahlgrad darstellen lassen.

In dieser Arbeit handelt es sich nur um zwei Probleme: (1) Wann enthält $PSL_n(q)$ eine Untergruppe von Primzahlindex? Dies wird in Satz 1 beantwortet. (2) Eine Gruppe $G = PSL_n(q)$ enthalte eine Untergruppe vom Primzahlindex l. Wie viele Klassen konjugierter Untergruppen vom Index l gibt es in G? Diese Frage wird in Satz 2 beantwortet.

Bezeichnungen. F_q: Galois-Feld mit q Elementen. $GL_n(q)$: die n-dimensionale volle lineare Gruppe über F_q. $SL_n(q)$: die n-dimensionale spezielle lineare Gruppe über F_q. $PSL_n(q) = SL_n(q)/\text{Zentrum}$: die n-dimensionale projektive spezielle lineare Gruppe über F_q.

§ 1.

Vorerst schicken wir einen Hilfssatz voraus:

Hilfssatz 1. *Sei G eine zweifach transitive Permutationsgruppe von Grade n und H eine Untergruppe von G, deren Index kleiner als n ist. Dann ist H transitiv.*

Beweis. Wir ordnen jeder Permutation von G ihre Permutationsmatrix zu und erhalten so die Permutationsdarstellung G^* von G. Sei χ^* der Charakter von G^*. Da G zweifach transitiv ist, zerfällt χ^* in den Hauptcharakter $1(G)$ von G und einen irreduziblen Charakter χ des Grades $n-1$ von G. ([4], (29. 9)). Sei s die Anzahl der Transitivitätsgebiete von H. Ist

$s=1$, dann sind wir fertig. Also sei $s>1$. Dann enthält χ^*, auf H eingeschränkt, den Hauptcharakter $1(H)$ von H mit der Vielfachheit s. Da $s>1$ ist, enthält χ auf H den Hauptcharakter $1(H)$ von H mit positiver Vielfachheit. Dann kommen nach dem Reziprozitätssatz von Frobenius χ und $1(G)$ in $1^*(H)$ wirklich vor. Da der Grad von $1^*(H)$ gleich $G:H$ ist, haben wir die Ungleichung $G:H \geqq 1+n-1=n$, was unsere Annahme $G:H<n$ widerspricht.

Satz 1. *Sei $q=p^s$ eine Primzahlpotenz, $n\geqq 2$ und $q>3$ für $n=2$. $PSL_n(q)$ enthalte eine Untergruppe vom Primzahlindex l. Dann gilt die Gleichung $l=\frac{q^n-1}{q-1}$. Insbesondere ist $n=r$ eine Primzahl, s wird eine Potenz von r und es gilt $q\not\equiv 1 \pmod r$. Es gibt drei Ausnahmen, die für $n=2$ und für $q=5, 7$ und 11 auftreten.*

Beweis. Wir betrachten $G=SL_n(q)$. Bekanntlich ist die Ordnung von G gleich $q^{\frac{n(n-1)}{2}}(q^n-1)\cdots(q^2-1)$ ([1], §99). Nach Voraussetzung enthält G eine Untergruppe H vom Index l. Sei $Z=Z_n(q)$ das Zentrum von G. Dann besteht Z aus allen Matrizen der Gestalt $\begin{pmatrix}\mu & & & \\ & \mu & & \\ & & \ddots & \\ & & & \mu\end{pmatrix}$ mit $\mu^n=1$, $\mu\in F_q$. Also hat Z die Ordnung $d=(n, q-1)$. Da G/Z bekanntlich einfach ist ([1], § 104), ist die Permutationsgruppe (G, H) über den rechtsseitigen Nebenklassen von G nach H zu G/Z isomorph. Also haben wir die folgende Aussage:

(*) Die Primzahl l teilt die Ordnung von G/Z zur ersten Potenz und jede Restklasse LZ $(L\in SL_n(q))$ der Ordnung l ist nur mit ihrer Potenzen vertauschbar.

Fall I: $l\neq p$. Sei $m>0$ die kleinste Zahl, die der Kongruenz $q^m\equiv 1 \pmod l$ genügt. Angenommen, es sei $m<n-1$. Dann gilt $m>1$. Denn wegen $n-1>m$ ist die Ordnung von G durch $(q^3-1)(q^2-1)$ teilbar. Also wenn $m=1$ ist, muß l in d aufgehen. Sonst teilt l die Ordnung von G/Z in höherer als der ersten Potenz. Sei also $d\equiv 0 \pmod l$. Wegen der Einfachheit von G/Z ist l nicht kleiner als 5. Da $n\equiv 0 \pmod d$ ist, folgt $n\equiv 0 \pmod l$, insbesondere $n\geqq 5$. Dann teilt l die Ordnung von G/Z wieder in höhere als der ersten Potenz. Das widerspricht (*). Daher ist $m>1$. Dann gibt es in G eine Matrix L der Ordnung l der Gestalt $L=\begin{pmatrix}E & 0\\ 0 & L_m\end{pmatrix}$ mit $L_m\in SL_m(q)$. L ist mit jeder Matrix aus G der Gestalt $A=\begin{pmatrix}A_{n-m} & 0\\ 0 & E\end{pmatrix}$ mit $A_{n-m}\in SL_{n-m}(q)$ vertauschbar. Das widerspricht (*).

Nun sei $m=n-1$ und $m>1$. Man setze $F_{q^m}=\langle\lambda\rangle$ und $f(x)=$ $=(x-\lambda)(x-\lambda^q)\cdots(x-\lambda^{q^{m-1}})=x^m-a_1x^{m-1}-\cdots-a_m$ mit $a_i\in F_q$. Es sind $\begin{pmatrix}\lambda & & & \\ & \lambda^q & & \\ & & \ddots & \\ & & & \lambda^{q^{m-1}}\end{pmatrix}$ und $A=\begin{pmatrix}a_1 & \cdots & a_{m-1} & a_m \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}$ in $GL_n(q^m)$ konjugiert. Dann gehört $L=\begin{pmatrix}A^{q-1} & 0 \\ 0 & 1\end{pmatrix}$ zu G und hat die Ordnung $\frac{q^m-1}{q-1}$. Nach (*) folgt daraus die Gleichung $\frac{q^m-1}{q-1}=l$. Sei G_1 die Untergruppe aller Matrizen der Gestalt $\begin{pmatrix}a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}$ aus G. Dann ist der Index von G_1 in G gleich $\frac{q^n-1}{q-1}=ql+1$. Wegen $(ql+1,l)=1$ gilt $G=G_1H$. Setze $H_1=H\cap G_1$. Dann gilt $G_1:H_1=l$. G_1 enthält einen elementar abelschen Normalteiler N der Ordnung $q^m=(q-1)l+1$, der aus allen Matrizen der Gestalt $\begin{pmatrix}1 & 0 & \cdots & 0 \\ a_{21} & & & \\ \vdots & & E & \\ a_{n1} & & & \end{pmatrix}$ von G besteht. Sei L eine l-Sylowgruppe von G_1. Daraus folgt $N^L=N\subseteqq H_1\subseteqq H$. Nun haben wir $G=LH$. Also enthält der Durchschnitt aller Konjugierten von H in G die Untergruppe $N>1$. Das widerspricht der Einfachheit von G.

Nun sei $m=1$ und $n=2$. Man setze $F_q=\langle\lambda\rangle$ und $L=\begin{pmatrix}\lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix}$. Dann hat LZ die Ordnung $q-1$ für $p=2$ und $\frac{q-1}{2}$ für $p>2$. Nach (*) gilt die Gleichung $l=q-1$ für $p=2$ und $l=\frac{q-1}{2}$ für $p>2$. Also besitzt H/Z die Ordnung $q(q+1)$. Da je zwei verschiedene p-Sylowgruppen von $GL_2(q)$ den Durchschnitt E haben, ist die Anzahl der p-Sylowgruppen von H/Z kongruent 1 (mod q) und daher enthält H/Z, nach dem Sylowschen Satz oder nach einem Satz von FROBENIUS ([4], (5.1)), einen Normalteiler N/Z der Ordnung q oder $q+1$. Wenn die Ordnung von N/Z gleich q ist, so ist N/Z nach dem Sylowschen Satz ein Normalteiler von G/Z, was der Einfachheit von G/Z widerspricht. Also ist die Ordnung von N/Z gleich $q+1$. Wenn H/Z keinen Normalteiler der Ordnung q besitzt, da je zwei verschiedene p-Sylowgruppen

von H/Z den Durchschnitt E haben, gibt es kein Element $(\neq 1)$ in einer p-Sylowgruppe von H/Z, das mit einem Element $(\neq 1)$ von N/Z vertauschbar ist. Also sind alle Elemente $(\neq 1)$ von N/Z in H/Z konjugiert und N/Z ist eine elementar abelsche Gruppe von Primzahlpotenzordnung und eine p-Sylowgruppe von H/Z ist zyklisch (vgl. [5], Satz 3). Daraus folgt $q=p$. Da l der größte Primzahlteiler der Ordnung von G/Z sein muß, ist das ein Widerspruch.

Schließlich sei $m=n$. Wir setzen wieder $F_{q^n}=\langle\lambda\rangle$ und $f(x)=$ $=(x-\lambda)(x-\lambda^q)\cdots(x-\lambda^{q^{n-1}})=x^n-a_1x^{n-1}-\cdots-a_n$ mit $a_i\in F_q$. Dann sind $\begin{pmatrix}\lambda & & & \\ & \lambda^q & & \\ & & \ddots & \\ & & & \lambda^{q^{n-1}}\end{pmatrix}$ und $A=\begin{pmatrix}a_1 & \cdots & a_{n-1} & a_n\\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}$ in $GL_n(q^n)$ konjugiert. Da $\det A=\lambda^{\frac{q^n-1}{q-1}}$ ist, enthält G/Z ein Element der Ordnung $\frac{q^n-1}{d(q-1)}$. Nach (*) folgt daraus die Gleichung $l=\frac{q^n-1}{d(q-1)}$. Indem wir einen Satz von ZSIGMONDY [6] benützen, sehen wir leicht ein, daß $n=r$ eine Primzahl ist. Daraus folgt, daß $d=(r,q-1)$ gleich entweder 1 oder r ist. Zunächst sei $d=r$. Wieder sei G_1 die Untergruppe aller Matrizen der Gestalt $\begin{pmatrix}a_{11} & 0 & \cdots & 0\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \vdots & \vdots & & \vdots\\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}$ aus G. Dann ist der Index von G_1 in G gleich $\frac{q^r-1}{q-1}=lr$. Sei E_r ein r-dimensionaler Vektorraum über F_q. Dann kann man $G/Z=$ $=PSL_r(q)$ als eine Permutationsgruppe über der Menge aller eindimensionalen Unterräume von E_r betrachten. Dabei wird G_1/Z die Untergruppe derjenigen Elemente von G/Z, die die „Ziffer" $\langle(1,0,\ldots,0)\rangle$ festlassen. Diese Permutationsgruppe G/Z ist bekanntlich zweifach transitiv. Also ist nach Hilfssatz 1 H/Z transitiv. Daher haben wir $G=G_1H$. Daraus folgt $G_1:G_1\cap H=$ $=G:H=l$. Da die Ordnung von G_1 prim zu l ist, ist das ein Widerspruch. Also haben wir $d=1$.

Wäre $q\equiv 1 \pmod r$, dann würde $l=q^{r-1}+\cdots+1\equiv r\equiv 0 \pmod r$, $l=r$ und $q^{r-1}=1$ folgen. Also gilt die Inkongruenz $q\not\equiv 1 \pmod r$.

Es ist $\frac{p^{sr}-1}{p^s-1}=l$. Wäre s keine Potenz von r, so gäbe es einen echten Teiler t von sr, der kein Teiler von s ist. Nach einem Satz von ZSIGMONDY [6] gibt es eine Primzahl u, für die p zum Exponenten gehört. Dann würde u ein Teiler von l. Also muß s eine Potenz von r sein.

Fall II: $l=p$. Dann folgt unmittelbar $n=2$ und $q=p$ (vgl. (*)). Dann ist unsere Behauptung schon bekannt ([1], § 262). Doch möchten wir hier einen anderen Beweis angeben.

Sei $p\equiv 1 \pmod 4$. Nach einem Satz von BURNSIDE ([4], (11.7)) ist die Permutationsdarstellung (G, H) zweifach transitiv. Also enthält H eine Untergruppe K von Index $p-1$. Dann ist die Ordnung von K/Z gleich $(p+1)/2$ und daher ist K/Z eine Hall-Untergruppe von G/Z. Da G (wie oben) ein Element der Ordnung $p+1$ enthält, ist K/Z, nach einem Satz von WIELANDT [3], zyklisch. Wie oben ist K in $GL_2(p^2)$ mit $\left\langle \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^p \end{pmatrix}; \lambda^{p+1}=1 \right\rangle$ konjugiert. Sei $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \lambda^i & 0 \\ 0 & \lambda^{pi} \end{pmatrix}=\begin{pmatrix} \lambda^j & 0 \\ 0 & \lambda^{pj} \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit $\lambda^i \neq \lambda^j$ und $ad-bc=1$. Dann folgt $a=d=0$ und $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Andererseits ist jedes Element von G, dessen Ordnung gleich 4 oder ein Primteiler von $p(p-1)$ ist, zu einer Matrix der Gestalt $\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}$ konjugiert (in G). Sei $\begin{pmatrix} c & d \\ e & f \end{pmatrix}\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}=\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}\begin{pmatrix} c & d \\ e & f \end{pmatrix}$ mit $cf-de=1$ und $b\neq 0$ oder $a\neq a^{-1}$. Dann folgt $d=0$. Also ist die Ordnung von $\begin{pmatrix} c & d \\ e & f \end{pmatrix}$ ein Teiler von $p(p-1)$. Nun sei r ein Primteiler von $\frac{p+1}{2}$ und $K(r)$ die r-Sylowgruppe von K. Also ist jedes Element $(\neq 1)$ von $K(r)$ mit einem Element A von G, dessen Ordnung $p(p-1)$ teilt, nur dann vertauschbar, wenn $A=\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ist. Es sei $N(r)$ der Normalisator von $K(r)$ in G. Dann ist wegen der Einfachheit von G und nach dem Zerfällungssatz von BURNSIDE $N(r)\neq K$. Daher hat $N(r)$ die Ordnung $2(p+1)$. Wenn also $N(r)$ in H enthalten ist, haben wir, nach dem Sylowschen Satz, die Kongruenz $\frac{p-1}{2}\equiv 1 \pmod r$. Daraus folgt $p\equiv 3 \pmod r$. Da andererseits $p\equiv -1 \pmod r$ ist, folgt der Widerspruch $r=2$. Daher haben wir $N(r)\cap H=K$ und H/Z ist eine Frobeniusgruppe. Also umfaßt H/Z, nach einem Satz von FROBENIUS ([4], (5.1)), einen Normalteiler N/Z der Ordnung $p-1$ und alle von Eins verschiedenen Elemente von N/Z sind in H/Z konjugiert. Daraus folgt die Gleichung $p-2=\frac{p+1}{2}$ und $p=5$. Umgekehrt enthält $PSL_2(5)\cong A_5$ eine Untergruppe vom Index 5.

Sei $p\equiv 3 \pmod 4$. G_1 bezeichne die Untergruppe von G, die aus allen Matrizen der Gestalt $\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}$ besteht. Da der Index von G_1 in G gleich $p+1$

ist, haben wir $G = HG_1$ und $H:G_1 \cap H = G:G_1 = p+1$. Also enthält H eine Untergruppe K vom Index $p+1$. Dann ist die Ordnung von K/Z gleich $\frac{p-1}{2}$ und daher ist K/Z eine Halluntergruppe von G/Z. Da G ein Element der Ordnung $p-1$ enthält, ist K/Z nach einem Satz von WIELANDT [3] zyklisch. Andererseits enthält H wie im Falle $p \equiv 1 \pmod 4$ eine Untergruppe L vom Index $p-1$. Dann ist die Ordnung von L/Z gleich $\frac{p+1}{2}$.

G_2 sei die Untergruppe von G, die aus allen Matrizen der Gestalt $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ besteht. Sei m die Anzahl aller Involutionen in G/Z und m_1 und m_1' diejenigen in G_1/Z und in H/Z. Da (G, G_1) und (G, H) zweifach transitiv sind, gibt es Involutionen $\bar{I}(=IZ)$ und $\bar{I}'(=I'Z)$, die im Normalisator von G_2/Z bzw. von L/Z liegen, mit den Gleichungen $G/Z = G_1/Z + (G_1/Z)\,\bar{I}(G_1/Z)$ und $G/Z = H/Z + (H/Z)\,\bar{I}'(H/Z)$. Seien d und d' die Anzahlen der Elemente X in G_2/Z und in L/Z mit den Gleichungen $\bar{I}\bar{X}\bar{I} = \bar{H}^{-1}$ und $\bar{I}'\bar{X}\bar{I}' = \bar{X}^{-1}$. Dann bekommen wir die Gleichungen (vgl. [2]) $m = m_1 + pd = m_1' + (p-1)\,d'$. Da die Ordnung von G_1/Z ungerade ist, haben wir $m_1 = 0$. Der Normalisator von G_2/Z ist gleich $G_2\langle I\rangle/Z$; er ist also eine Diedergruppe. Daher enthält $G_2\langle I\rangle/Z$ genau $\frac{p-1}{2}$ Involutionen, und alle Involutionen in $G_2\langle I\rangle/Z$ sind konjugiert. Also haben wir $d = \frac{p-1}{2}$. Wir setzen $\alpha_1 = \langle(1\ 0)\rangle$ und $\alpha_2 = \langle(0,\ 1)\rangle$. Dann besitzt jede Involution in $G_2\langle I\rangle/Z$ die Zyklendarstellung $(\alpha_1\,\alpha_2)\cdots$. Da (G, G_1) zweifach transitiv ist, sind alle Involutionen in G/Z zu einander konjugiert. Nun haben wir die Gleichung $m_1' + (p-1)\,d' = \frac{p(p-1)}{2}$. Wir betrachten die Permutationsgruppe (G, H). Sei r die Anzahl der Ziffern, die bei einer Involution festbleiben. Da alle Involutionen konjugiert sind und da m' gleich der Anzahl aller Involutionen in G/Z ist, die „die Ziffer H/Z" festlassen, so haben wir die Gleichung $pm_1' = rm = \frac{rp(p-1)}{2}$. (Eine Ziffer wird bei m' Involutionen festgelaßen und es gibt p Ziffern. Eine Involution läßt r Ziffern fest und es gibt m Involutionen.)

G_2 liegt im Normalisator der p-Sylowgruppe $\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$ von G. Nach einem Satz von WIELANDT [3] sind K/Z und G_2/Z konjugiert. Also liegt K im Normalisator einer p-Sylowgruppe von G. Daraus folgt, daß jede Permutation $(\neq 1)$ von K/Z genau eine Ziffer (H/Z) festläßt und K/Z genau zwei Transitivitätsgebiete der Länge $\frac{p-1}{2}$ besitzt. Sei $N(K)$ der Normalisator von K in G. Dann haben wir $N(K) \subseteqq H$. Der Normalisator von G_2/Z

ist gleich $G_2\langle I\rangle/Z$. Sei $\bar{I}''=I''Z$ eine Involution in $N(K)/Z$. Da K Zentralisator jedes Elementes $\left(\neq\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\right)$ von K ist und K/Z genau zwei Transitivitätsgebiete der Länge $\frac{p-1}{2}$ besitzt, läßt $\bar{I}''$ genau 3 Ziffern fest. Also haben wir $r=3$ und $m'=\frac{3(p-1)}{2}$. Folglich haben wir $d'=\frac{p-3}{2}$. Daher gibt es in L/Z genau zwei Elemente $\bar{X}$ mit der Eigenschaft $\bar{I}'\bar{X}\bar{I}'\neq\bar{X}^{-1}$. Also ist die Ordnung von $\bar{X}$ höchstens gleich 4.

Sei M eine 2-Sylowgruppe von L derart, daß $M\langle I'\rangle$ eine 2-Sylowgruppe von G ist. $M\langle I'\rangle$ ist eine verallgemeinerte Quaternionengruppe, da bekanntlich $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ die einzige Involution in G ist. Also ist $M\langle I'\rangle/Z$ eine Diedergruppe. Wir setzen $\frac{p+1}{2}=2^{\alpha}u$ mit $(2,u)=1$. Dann wird $M\langle I'\rangle/Z$ durch zwei Elemente $\bar{A}$ und $\bar{B}$ mit $\bar{A}^{2^{\alpha}}=\bar{B}^2=1$ und $\bar{B}\bar{A}\bar{B}=\bar{A}^{-1}$ erzeugt. Man kann $\bar{I}'=\bar{B}\bar{A}^{\alpha}$ setzen.

Wenn $M/Z=\langle\bar{A}\rangle$ ist, gilt für jedes Element $\bar{X}$ aus M/Z die Gleichung $\bar{I}'\bar{X}\bar{I}'=\bar{X}^{-1}$. Also gibt es in L/Z ein Element $\bar{Y}$ der Ordnung 3, für das die Ungleichung $\bar{I}'\bar{Y}\bar{I}'\neq\bar{Y}^{-1}$ gilt. Wegen $\bar{I}'(\bar{I}'\bar{Y}\bar{I}')\bar{I}'=\bar{Y}$ folgt daraus $\bar{I}'\bar{Y}\bar{I}'=\bar{Y}$. Wegen $\bar{A}^{x}\bar{Y}\neq\bar{Y}^{\pm1}$ für $\bar{A}^{x}\neq1$ folgt weiter $\bar{I}'\bar{A}^{x}\bar{Y}\bar{I}'=\bar{Y}^{-1}\bar{A}^{-x}=\bar{A}^{-x}\bar{Y}$. Insbesondere gilt $\bar{Y}^{-1}\bar{A}^{-1}=\bar{A}^{-1}\bar{Y}$. Wenn $a\geqq2$ ist, folgt daraus $\bar{A}^2\bar{Y}=\bar{Y}\bar{A}^2$. Das widerspricht $\bar{Y}^{-1}\bar{A}^{-2}=\bar{A}^{-2}\bar{Y}$. Also haben wir $a=1$. Wenn $\{\bar{A}\}\{Y\}\neq L/Z$ ist, sei $\bar{Y}'$ ein Element aus $L/Z-\{\bar{A}\}\{\bar{Y}\}$, das eine zu 2 teilerfremde Ordnung hat. Wegen $\bar{Y}'\bar{Y}\neq\bar{Y}^{\pm1}$ ist, gilt $\bar{I}'\bar{Y}'\bar{Y}\bar{I}'=\bar{Y}^{-1}\bar{Y}'^{-1}=\bar{Y}'^{-1}\bar{Y}$. Dann muß die Ordnung von $\bar{Y}'$ gerade sein. Das ist ein Widerspruch. Also ist $L/Z=\{\bar{A}\}\{\bar{Y}\}$ und $\frac{p+1}{2}=6$, das heißt $p=11$.

Wenn $M/Z\neq\langle\bar{A}\rangle$ ist, gibt es in M/Z $2^{\alpha-1}$ Elemente der Gestalt $\bar{B}\bar{A}^{x}$. Für diese Elemente gilt $\bar{B}\bar{A}^{\alpha}\bar{B}\bar{A}^{x}\bar{B}\bar{A}^{\alpha}=\bar{B}\bar{A}^{2\alpha-x}\neq\bar{B}\bar{A}^{x}=(\bar{B}\bar{A}^{x})^{-1}$. Also haben wir $2^{\alpha-1}\leqq2$, daß heißt $a\leqq2$. Wenn $a=1$ ist, kann man annehmen, daß $M/Z=\langle\bar{A}\rangle$ ist. Also haben wir $a=2$ und $M/Z=\langle\bar{A}^2,\bar{B}\bar{A}^{\beta}\rangle$. Dann gilt $\bar{I}'\bar{B}\bar{A}^{\beta}\bar{I}'=\bar{B}\bar{A}^{\beta+2}$. Nun sei $\bar{X}\neq1$ ein Element aus L/Z mit einer ungeraden Ordnung. Wegen $\bar{B}\bar{A}^{\beta}\bar{X}\neq\bar{B}\bar{A}^{\beta},\bar{B}\bar{A}^{\beta+2}$ haben wir $\bar{I}'\bar{B}\bar{A}^{\beta}\bar{X}\bar{I}'=\bar{X}^{-1}\bar{B}\bar{A}^{\beta}=\bar{B}\bar{A}^{\beta+2}\bar{X}^{-1}$. Wegen $\bar{A}^2\bar{X}\neq\bar{B}\bar{A}^{\beta},\bar{B}\bar{A}^{\beta+2}$ haben wir ferner $\bar{I}'\bar{A}^2\bar{X}\bar{I}'=\bar{X}^{-1}\bar{A}^2=\bar{A}^2\bar{X}^{-1}$. Daraus folgt $\bar{X}^{-2}\bar{B}\bar{A}^{\beta}\bar{X}^2=\bar{B}\bar{A}^{\beta}$. Da die Ordnung von $\bar{X}$ ungerade ist, folgt daraus $\bar{X}^{-1}\bar{B}\bar{A}^{\beta}\bar{X}=\bar{B}\bar{A}^{\beta}$. Das ist ein Widerspruch. Also gibt es kein Element $\bar{X}\neq1$ aus L/Z mit einer ungeraden Ordnung. Deshalb haben wir $L/Z=M/Z$ und $\frac{p+1}{2}=4$, das heißt $p=7$.

Umgekehrt betrachten wir $SL_2(3)$ (und $SL_2(5)$). Da die Ordnung von $SL_2(3)$ gleich $48 \not\equiv 0 \pmod 7$ ist, hat $SL_2(3)$ zwei irreduzible treue Darstellungen des Grades 2 über einem algebraisch abgeschlossenen Körper der Charakteristik 7. Die Charaktere dieser Darstellungen liegen in F_7. Also enthält $SL_2(7)$ zwei nicht konjugierte $SL_2(3)$. Ebenso enthält $SL_2(11)$ zwei nicht konjugierte $SL_2(5)$.

Damit ist der Beweis von Satz 1 beendet.

§ 2.

Wir schicken einige Hilfssätze voraus:

Hilfssatz 2. *Wenn $n>2$ ist, so ist die Bedingung*

$$\left((q^{n-1}-1)\cdots(q^2-1),\ \frac{q^n-1}{q-1}\right)=1$$

äquivalent mit den Aussagen: (1) *n ist eine Primzahl und* (2) $q \not\equiv 1 \pmod n$.

Beweis. Wenn n nicht prim ist, setzen wir $n=n_1n_2$ mit $n_i>1$ $(i=1,2)$. Dann haben wir $\frac{q^n-1}{q-1}=\frac{q^{n_1n_2}-1}{q-1}=\frac{q^{n_1n_2}-1}{q^{n_1}-1}\cdot\frac{q^{n_1}-1}{q-1}$. Also teilt jeder Primteiler von $\frac{q^{n_1}-1}{q-1}$ gleichzeitig $(q^{n-1}-1)\cdots(q-1)$ und $\frac{q^n-1}{q-1}$. Daher ist $n=r$ eine Primzahl. Wenn $q\equiv 1 \pmod r$ ist, haben wir $\frac{q^r-1}{q-1}=$ $=q^{r-1}+\cdots+1\equiv r\equiv 0 \pmod r$. Also teilt r gleichzeitig $(q^{r-1}-1)\cdots(q^2-1)$ und $\frac{q^r-1}{q-1}$.

Umgekehrt sei n eine Primzahl und $q \not\equiv 1 \pmod n$. Sei l ein gemeinsamer Primteiler von $\frac{q^n-1}{q-1}$ und $(q^{n-1}-1)\cdots(q^2-1)$. Dann folgt $q^n\equiv 1 \pmod l$ und $q^x\equiv 1 \pmod l$ mit $x<n$. Da n prim ist, haben wir $q\equiv 1 \pmod l$. Deshalb haben wir $\frac{q^n-1}{q-1}\equiv n\equiv 0 \pmod l$ und $n=l$. Das ist ein Widerspruch.

Aus diesem Hilfssatze folgt unmittelbar der folgende

Hilfssatz 3. *Es sei $G=SL_n(q)$. G_1 bezeichne die Untergruppe von G, die aus allen Matrizen der Gestalt* $\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ *besteht. G_1 ist genau dann eine Hall-Gruppe von G, wenn* (1) *n eine Primzahl ist und* (2) $q \not\equiv 1 \pmod n$.

Wir bemerken noch, daß in diesem Falle $Z=1$ ist. In der Tat ist die Ordnung von Z gleich $(n, q-1)=1$. Also haben wir $SL_n(q) \cong PSL_n(q)$.

Wir brauchen noch einen Hilfssatz:

Hilfssatz 4. *Sei $G=SL_n(q)$ und K eine über F_q irreduzible Untergruppe von G, die eine p-Sylowgruppe P von G enthält, wobei $q=p^s$ ist. Dann ist K transitiv, wenn man G als Permutationsgruppe auf der Menge aller eindimensionalen Unterräume des n-dimensionalen Vektorraumes $E_n(q)$ über F_q betrachtet.*

Beweis. Man kann annehmen, daß P aus allen Matrizen der Gestalt $\begin{pmatrix} 1 & & & \\ x_{21} & 1 & & \\ \vdots & & \ddots & \\ x_{n1} & & & 1 \end{pmatrix}$ besteht. Zunächst bestimmen wir die Transitivitätsgebiete von P. Sei T_k die Menge aller eindimensionalen Teilräume von $E_n(q)$, die eine Erzeugende der Gestalt $(x_1, \ldots, x_k, 0, \ldots, 0)$ mit $x_k \neq 0$ besitzen. Dann sind $T_1, T_2, \ldots, T_n$ die Transitivitätsgebiete von P. In der Tat haben wir $(0, \ldots, \overset{k}{\overset{\vdots}{0}}, 1, 0, \ldots, 0) \begin{pmatrix} 1 & & & \\ x_{21} & 1 & & \\ \vdots & & \ddots & \\ x_{n1} & & & 1 \end{pmatrix} = (x_{k1}, \ldots, x_{k\,k-1}, 1, 0, \ldots, 0)$. Nun läßt K die Vereinigungsmenge von $T_{i_1}, \ldots, T_{i_l}$ $(1 \leqq i_1 < \cdots < i_l < n)$ nicht fest. Denn setzen wir für jedes A aus K $A=\begin{pmatrix} \overset{i_l}{\boxed{B}}\,{}^{i_l} & C \\ D & F \end{pmatrix}$, dann folgt aus $(x_1, \ldots, x_{i_l}, 0, \ldots, 0) \begin{pmatrix} B & C \\ D & F \end{pmatrix} = (y_1, \ldots, y_{i_l}, 0, \ldots, 0)$, wobei x_j alle Elemente von F_q durchläuft $(j=1, \ldots, i_l)$, daß $C=0$ ist. Aber da K irreduzibel ist, gibt es ein A in K mit $C \neq 0$:

Satz 2. *Es sei $G=SL_n(q)$, $n>2$ eine Primzahl $q \not\equiv 1 \pmod{n}$. Dann enthält G genau zwei Klassen konjugierter Hall-Gruppen vom Index $\frac{q^n-1}{q-1}$.*

Beweis (I). Es gibt mindestens zwei Klassen konjugierter Hall-Untergruppen vom Index $\frac{q^n-1}{q-1}$. Sei G_1 die Untergruppe von G, die aus allen Matrizen der Gestalt $A=\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ besteht. Wir ordnen jeder

Matrix A von G_1 die Matrix $(A')^{-1}$ zu, wobei A' die transponierte Matrix von A bezeichnet. Wegen $((AB)')^{-1}=(B'A')^{-1}=(A')^{-1}(B')^{-1}$ ist diese Abbildung ein Isomorphismus von G_1. Wir bezeichnen mit G_1^* das Bild von G_1. Betrachten wir G als Permutationsgruppe auf der Menge aller eindimensionalen Unterräume von $E_n(q)$, so ist G transitiv und G_1 ist die maximale Untergruppe von G, die die „Ziffer" $\langle(1, 0, \ldots, 0)\rangle$ festläßt. Nun ist G_1^* nicht zu G_1 konjugiert. Dazu genügt es zu zeigen, daß G_1^* keine „Ziffer" festläßt. G_1^* besteht aus allen Matrizen der Gestalt $\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix}$.

Angenommen, $\langle(x_1, x_2, \ldots, x_n)\rangle \neq 0$ wird von G_1^* festgelassen.

Die Matrizen $\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & a_{kk}=1 & 1=a_{k,k+1} & \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix}$ $(k=1, 2, \ldots, n-1)$ gehören G_1^*.

Aus $(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n)\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & a_{kk}=1 & 1=a_{k,k+1} & \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix}=$

$=(x_1, \ldots, x_k, x_k+x_{k+1}, x_{k+2}, \ldots, x_n)$ folgt $x_k=0$ $(k=1, \ldots, n-1)$.

Wegen $n>2$ enthält G_1^* die Matrix $\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & -1 \\ & & & 1 & 0 \end{pmatrix}$. Aus

$(0, \ldots, 0, x_n)\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & -1 \\ & & & 1 & 0 \end{pmatrix}=(0, \ldots, 0, x_n, 0)$ folgt $x_n=0$.

Das ist ein Widerspruch.

(II) Es gibt genau zwei Klassen konjugierter Hall-Untergruppen vom Index $\frac{q^n-1}{q-1}$. Sei H eine beliebige Untergruppe von G mit den Index

$\frac{q^n-1}{q-1}$. Dann enthält H eine p-Sylowgruppe von G. Wenn H irreduzibel in F_q ist, so ist H transitiv nach Hilfssatz 4. Dann ist die Ordnung von H durch $\frac{q^n-1}{q-1}$ teilbar. Das ist ein Widerspruch. Also ist H reduzibel in F_q. Daher kann man annehmen, daß jede Matrix A von H die folgende Gestalt hat: $A=\begin{pmatrix} A_1 & 0 \\ * & A_2 \end{pmatrix}$, wobei der Grad von A_i gleich n_i $(i=1,2)$ ist, unabhängig von A aus H. Wenn $1<n_1<n-1$ gilt, so sei m eine Primzahl, die die Bedingung $q^{n-1}\equiv 1 \pmod m$, $q^\nu \not\equiv 1 \pmod m$ für $1 \leqq \nu < n-1$ erfüllt. Eine solche Primzahl existiert nach einem Satz von Zsigmondy [6], außer im Falle $q=2$ und $n=7$. Dann muß jedes Element der Ordnung m von H die folgende Gestalt haben: $\begin{pmatrix} E & 0 \\ * & E \end{pmatrix}$. Das ist ein Widerspruch. Daher ist $n_1=1$ oder $n_1=n-1$ und es gilt

$$\begin{pmatrix} & & -1 \\ 1 & \ddots & \\ & 1 & \\ 1 & & \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1\,n-1} & 0 \\ \vdots & & \vdots & \vdots \\ a_{n-1} & \cdots & a_{n-1\,n-1} & 0 \\ a_{n1} & \cdots & a_{n\,n-1} & a_{nn} \end{pmatrix} \begin{pmatrix} & & 1 \\ 1 & \ddots & \\ & 1 & \\ -1 & & \end{pmatrix} = \begin{pmatrix} a_{nn} & & \\ 0 & & \\ & & * \\ 0 & & \end{pmatrix}.$$

Also ist H außer im Falle $q=2$ und $n=7$ entweder zu G_1 oder zu G_1^* konjugiert. Nun sei $q=2$ und $n=7$. Die Ordnung der Untergruppe, die aus allen Matrizen der Gestalt $\begin{pmatrix} \text{Grad } 2 & 0 \\ * & \text{Grad } 5 \end{pmatrix}$ besteht, ist nicht durch 7 teilbar. Weiter ist die Ordnung der Untergruppe, die aus allen Matrizen der Gestalt $\begin{pmatrix} \text{Grad } 3 & 0 \\ * & \text{Grad } 4 \end{pmatrix}$ besteht, nicht durch 31 teilbar. Andererseits ist die Ordnung von H durch $7\cdot 31$ teilbar. Daher gilt wieder $n_1=1$ oder $n_1=6$ und wir können den obigen Schluß wiederholen.

Damit ist der Beweis von Satz 2 beendet.

Sei $n=2$. Da dann G_1 und G_1^* zueinander konjugiert sind, gibt es nach Teil (II) des vorangegangenen Beweis nur eine einzige Klasse von Hall-Untergruppen vom Index $q+1$.

Nun fragen wir „wie stark transitiv" die Permutationsgruppen (G, G_1) sind. Nach BURNSIDE sind sie zweifach transitiv. Für $n>2$ sind sie aber nicht zweifach primitiv, das heißt, G_1 ist nicht primitiv als Permutationsgruppe auf den von $\langle(1,0,\ldots,0)\rangle$ verschiedenen Ziffern. Zum Beispiel besteht die Untergruppe G_2, die die Ziffern $\langle(1,0,\ldots,0)\rangle$ und $\langle(0,1,\ldots,0)\rangle$ festläßt, aus allen Matrizen der Gestalt $\begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ 0 & a_{22} & 0 & \cdots & 0 \\ & & * & & \end{pmatrix}$. Sie ist enthalten in der

Untergruppe von G_1, die aus allen Matrizen der Gestalt $\begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ & & * & & \end{pmatrix}$ besteht; G_2 ist also keine maximale Untergruppe von G_1. Für $n=2$ und $q=2^s$ ist (G, G_1) bekanntlich dreifach transitiv. In Zusammenhang mit dieser Betrachtung und Satz 2 teilen wir den folgenden Satz mit:

Satz 3. *Sei G eine dreifach transitive Permutationsgruppe des Grades n auf der Menge $\{1, \ldots, n\}$ und H eine intransitive Untergruppe vom Index n. Dann ist $H=G_i$ für ein passendes i. Dabei bezeichnet G_i die maximale Untergruppe von G, welche die Ziffer i festläßt.*

Beweis. Aus dem Beweis von Hilfssatz 1 in § 1 folgt, daß H genau zwei Transitivitätsgebiete T_1 und T_2 hat. Sei n_k die Länge von T_k und $n_1 \leqq n_2 = n - n_1$. Sei $i \in T_1$. Dann haben wir $G_i : G_i \cap H = HG_i : H = HG_i : G_i = n_1 \leqq n - n_1$. Sei $n_1 > 2$. Da G_i zweifach transitiv ist, ist $G_i \cap H$ transitiv auf $\{1, \ldots, n\} - \{i\}$ nach Hilfssatz 1. Das ist ein Widerspruch. Deshalb muß $n_1 = 1$, und also $H = G_i$ sein.

Insbesondere bekommt man

Satz 4. *Sei G eine dreifach transitive Permutationsgruppe vom Primzahlgrad p und H eine Untergruppe vom Index p. Dann läßt H eine Ziffer fest.*

Literatur

[1] L. E. Dickson, *Linear groups* (Leipzig, 1901).

[2] N. Itô, Normalteiler mehrfach transitiver Permutationsgruppen, *Math. Zeitschrift*, **70** (1958), 165—173.

[3] H. Wielandt, Zum Satz von Sylow, *Math. Zeitschrift*, **60** (1954), 407—408.

[4] H. Wielandt, *Vorlesungen über Permutationsgruppen.* Ausarbeitung von J. André, (Tübingen, 1955).

[5] H. Zassenhaus, Über endliche Fastkörper, *Abh. Math. Sem. Hamburg*, **11** (1936), 187—220.

[6] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. f. Math. u. Phys.*, **3** (1892), 265—284.

(Eingegangen am 1. Februar 1960)

MATHEMATISCHES INSTITUT DER UNIVERSITÄT NAGOYA,
NAGOYA-CHIKUSA, JAPAN

Hallgruppen mit ausgezeichnetem Repräsentantensystem

Von RUDOLF KOCHENDÖRFFER in Rostock (Deutschland)

Ladislaus Rédei zum 60. Geburtstag

Besitzt in der Nebenklassenzerlegung

$$\mathfrak{G} = \sum_{R \in \mathfrak{R}} \mathfrak{U} R$$

der Gruppe $\mathfrak{G}$ nach ihrer Untergruppe $\mathfrak{U}$ das Repräsentantensystem $\mathfrak{R}$ die Eigenschaft:

$$U^{-1} \mathfrak{R} U = \mathfrak{R} \quad \text{für jedes } U \text{ aus } \mathfrak{U},$$

so wird $\mathfrak{R}$ ein *ausgezeichnetes* Repräsentantensystem genannt. Auf Untergruppen, die ein ausgezeichnetes Repräsentantensystem besitzen, wird man bei Untersuchungen über den Schurschen Multiplikator geführt [3]. Jedoch scheint dieser Begriff auch für allgemeine Strukturuntersuchungen einige Bedeutung zu besitzen. So hat z. B. kürzlich G. ZAPPA [4] unter Benutzung dieses Begriffes einen wohlbekannten Satz von BURNSIDE wesentlich verallgemeinert. Zweck der vorliegenden Note ist es, den Begriff des ausgezeichneten Repräsentantensystems zu anderen gruppentheoretischen Begriffen in Verbindung zu setzen. So zeigt sich, daß nilpotente Untergruppen mit ausgezeichnetem Repräsentantensystem im Sinne von D. G. HIGMAN [2] *hyperfokal* sind. Infolgedessen läßt sich der Satz von ZAPPA unmittelbar aus einem Satz von HIGMAN folgern. Diese Überlegungen beziehen sich auf nilpotente Hallgruppen. Es ist unbekannt, ob ein analoger Satz auch für auflösbare Hallgruppen richtig ist. Daher sollen weiter einige zusätzliche Bedingungen angegeben werden, die eine Übertragung auf den Fall auflösbarer Hallgruppen ermöglichen.

Sämtliche im folgenden betrachteten Gruppen sind endlich.

I

Unter einer *Hallgruppe* der Gruppe $\mathfrak{G}$ versteht man eine Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$, deren Ordnung $|\mathfrak{H}|$ zu ihrem Index $[\mathfrak{G}:\mathfrak{H}]$ teilerfremd ist. Eine Verallgemeinerung eines Satzes von BURNSIDE ist folgender

Satz von Zappa. *Besitzt die nilpotente Hallgruppe $\mathfrak{H}$ von $\mathfrak{G}$ ein ausgezeichnetes Repräsentantensystem in $\mathfrak{G}$, so enthält $\mathfrak{G}$ einen Normalteiler $\mathfrak{N}$ mit $\mathfrak{G}=\mathfrak{H}\mathfrak{N}$ und $\mathfrak{H}\cap\mathfrak{N}=1$.*

Der Beweis von ZAPPA stützt sich auf eine Arbeit von R. BAER [1]. Wir wollen diesem Satz aus einem Ergebnis von HIGMAN herleiten.

Für eine Untergruppe $\mathfrak{U}$ von $\mathfrak{G}$ betrachte man die *Fokalreihe* $\mathfrak{U}\geqq\mathfrak{U}_1\geqq\mathfrak{U}_2\geqq\ldots$ von $\mathfrak{U}$ in $\mathfrak{G}$, die nach HIGMAN folgendermaßen definiert wird: $\mathfrak{U}_0=\mathfrak{U}$; $\mathfrak{U}_{i+1}=$ Erzeugnis aller in $\mathfrak{U}_i$ gelegenen Kommutatoren $U_i G U_i^{-1} G^{-1}$ mit $U_i\in\mathfrak{U}_i$, $G\in\mathfrak{G}$. Wird einmal $\mathfrak{U}_k=1$, so nennt man $\mathfrak{U}$ *hyperfokal* in $\mathfrak{G}$. Jede hyperfokale Untergruppe ist nilpotent. Ein wichtiges Ergebnis der Arbeit [2] ist der

Satz von Higman. *Ist $\mathfrak{H}$ eine hyperfokale Hallgruppe in $\mathfrak{G}$, so enthält $\mathfrak{G}$ einen Normalteiler $\mathfrak{N}$ mit $\mathfrak{G}=\mathfrak{H}\mathfrak{N}$ und $\mathfrak{H}\cap\mathfrak{N}=1$.*

Es sei nun $\mathfrak{U}$ eine Untergruppe von $\mathfrak{G}$ mit ausgezeichnetem Repräsentantensystem $\mathfrak{R}$. Für jedes $U\in\mathfrak{U}$ und jedes $R\in\mathfrak{R}$ gilt also $RU=UR_1$ mit $R_1\in\mathfrak{R}$. Um die Glieder der Fokalreihe von $\mathfrak{U}$ zu bestimmen, hat man die Kommutatoren $U_iGU_i^{-1}G^{-1}$ mit $U_i\in\mathfrak{U}_i$, $G\in\mathfrak{G}$ zu betrachten. Setzt man $G=UR$ mit $U\in\mathfrak{U}$, $R\in\mathfrak{R}$, so wird, weil $\mathfrak{R}$ ausgezeichnet ist,

$$U_iGU_i^{-1}G^{-1}=U_iURU_i^{-1}R^{-1}U^{-1}=U_iUU_i^{-1}U^{-1}R_1R_2^{-1}$$

mit $R_1, R_2\in\mathfrak{R}$. Dieser Kommutator liegt genau dann in $\mathfrak{U}_i$ wenn $R_1=R_2$ ist. Also wird $\mathfrak{U}_{i+1}$ von allen Kommutatoren $U_iUU_i^{-1}U^{-1}$ mit $U_i\in\mathfrak{U}_i$, $U\in\mathfrak{U}$ erzeugt. Das bedeutet aber: $\mathfrak{U}_i$ ist das i-te Glied der absteigenden Zentralreihe von $\mathfrak{U}$. Insbesondere ergibt sich:

Ist $\mathfrak{U}$ eine nilpotente Untergruppe mit ausgezeichnetem Repräsentantensystem, so ist $\mathfrak{U}$ hyperfokal.

Mithin folgt der Satz von ZAPPA aus dem Satz von HIGMAN.

Ist umgekehrt $\mathfrak{H}$ eine hyperfokale Hallgruppe, so besitzt $\mathfrak{H}$ nach dem Satz von HIGMAN ein ausgezeichnetes Repräsentantensystem, nämlich den Normalteiler $\mathfrak{N}$. Damit ist festgestellt:

Eine nilpotente Hallgruppe besitzt dann und nur dann ein ausgezeichnetes Repräsentantensystem, wenn sie hyperfokal ist.

Insbesondere besitzt eine Sylowgruppe genau dann ein ausgezeichnetes Repräsentantensystem, wenn sie hyperfokal ist. Weiter ergibt sich aus der Arbeit von HIGMAN: Dann und nur dann ist $\mathfrak{G}$ nilpotent, wenn jede Sylowgruppe ein ausgezeichnetes Repräsentantensystem besitzt.

II

Es ist unbekannt, ob der Satz von ZAPPA richtig bleibt, wenn man die Voraussetzung, daß $\mathfrak{H}$ nilpotent ist, durch eine schwächere ersetzt. Wir werden im folgenden von $\mathfrak{H}$ nur Auflösbarkeit voraussetzen, dafür aber an das ausgezeichnete Repräsentantensystem zusätzliche Forderungen stellen.

Satz 1. *Es sei $\mathfrak{H}$ eine auflösbare Hallgruppe von $\mathfrak{G}$ mit ausgezeichnetem Repräsentantensystem $\mathfrak{R}$. Jedes Element aus $\mathfrak{R}$ lasse sich als Produkt solcher Elemente darstellen, deren Ordnungen zu $|\mathfrak{H}|$ teilerfremd sind. Dann gibt es in $\mathfrak{G}$ einen Normalteiler $\mathfrak{N}$ mit $\mathfrak{G}=\mathfrak{H}\mathfrak{N}$ und $\mathfrak{H}\cap\mathfrak{N}=1$.*

Beweis. Wir setzen zur Abkürzung $[\mathfrak{G}:\mathfrak{H}]=n$, bezeichnen die Elemente aus $\mathfrak{R}$ mit $R_1,\dots R_n$ und haben dann

$$\mathfrak{G}=\sum_{\nu=1}^{n}\mathfrak{H}R_\nu.$$

Für ein Element

$$G=HR_\nu \qquad (H\in\mathfrak{H},\ R_\nu\in\mathfrak{R})$$

setzen wir $\underline{G}=H$. Dann läßt sich die Verlagerung $v(X)$ eines Elementes X aus $\mathfrak{G}$ nach $\mathfrak{H}$ folgendermaßen schreiben:

$$v(X)=\mathfrak{H}'\prod_{\nu=1}^{n}\underline{R_\nu X},$$

wobei $\mathfrak{H}'$ die Kommutatorgruppe von $\mathfrak{H}$ bedeutet. Da $\mathfrak{R}$ ausgezeichnet ist, wird für ein Element H aus $\mathfrak{H}$

$$R_\nu H=HR_{\nu'} \qquad (\nu=1,\dots,n)$$

mit $R_{\nu'}\in\mathfrak{R}$, d. h. $\underline{R_\nu H}=H$. Folglich ist

$$v(H)=\mathfrak{H}'H^n.$$

Da n zur Ordnung $|\mathfrak{H}|$ teilerfremd ist, treten sämtliche Nebenklassen von $\mathfrak{H}$ nach $\mathfrak{H}'$ als Werte $v(H)$ mit passenden $H\in\mathfrak{H}$ auf, und genau für die Elemente H' aus $\mathfrak{H}'$ wird $v(H')=\mathfrak{H}'$.

Diejenigen Elemente aus $\mathfrak{G}$, die bei der Verlagerung auf $\mathfrak{H}'$ abgebildet werden, bilden einen Normalteiler $\mathfrak{G}_1$ von $\mathfrak{G}$. Nach dem oben Bemerkten ist

$\mathfrak{G} = \mathfrak{H}\mathfrak{G}_1$ und $\mathfrak{H} \cap \mathfrak{G}_1 = \mathfrak{H}'$. Da sich jedes Element aus $\mathfrak{R}$ als Produkt solcher Elemente darstellen läßt, deren Ordnungen zu $|\mathfrak{H}|$ teilerfremd sind, und da die Verlagerung eine homomorphe Abbildung auf $\mathfrak{H}/\mathfrak{H}'$ darstellt, wird $v(R_\nu) = \mathfrak{H}'$ für jedes $R_\nu \in \mathfrak{R}$. Folglich bildet $\mathfrak{R}$ ein ausgezeichnetes Repräsentantensystem für $\mathfrak{H}'$ in $\mathfrak{G}_1$:

$$\mathfrak{G}_1 = \sum_{\nu=1}^{n} \mathfrak{H}' R_\nu .$$

Mithin treffen auf die Gruppe $\mathfrak{G}_1$ wieder die Voraussetzungen des Satzes 1 zu.

Ist $\mathfrak{H}$ insbesondere abelsch, also $\mathfrak{H}' = 1$, so lehren die soeben angestellten Überlegungen, daß $\mathfrak{G}_1 = \mathfrak{R}$ ein Normalteiler in $\mathfrak{G}$ ist und $\mathfrak{G} = \mathfrak{H}\mathfrak{R}$ mit $\mathfrak{H} \cap \mathfrak{R} = 1$. Also ist Satz 1 für abelsche Hallgruppen gewiß richtig. Damit können wir einen Induktionsschluß nach der Anzahl der von 1 verschiedenen höheren Kommutatorgruppen der auflösbaren Gruppe $\mathfrak{H}$ beginnen. Dieser Induktionssluß liefert die Existenz eines Normalteilers $\mathfrak{N}$ von $\mathfrak{G}_1$ mit $\mathfrak{G}_1 = \mathfrak{H}'\mathfrak{N}$ und $\mathfrak{H}' \cap \mathfrak{N} = 1$. Wegen $\mathfrak{G} = \mathfrak{H}\mathfrak{G}_1$ wird $\mathfrak{G} = \mathfrak{H}\mathfrak{N}$. Weiter ist

$$\mathfrak{G}/\mathfrak{G}_1 \cong \mathfrak{H}/\mathfrak{H} \cap \mathfrak{G}_1 = \mathfrak{H}/\mathfrak{H}',$$

so daß $|\mathfrak{N}| = n$ und mithin auch $\mathfrak{H} \cap \mathfrak{N} = 1$ wird. Zu zeigen bleibt noch, daß $\mathfrak{N}$ sogar Normalteiler in $\mathfrak{G}$ ist, d. h. $H^{-1}\mathfrak{N}H = \mathfrak{N}$ für jedes $H \in \mathfrak{H}$. Für beliebige Elemente $N \in \mathfrak{N}$ und $H \in \mathfrak{H}$ wird, da $\mathfrak{G}_1$ Normalteiler in $\mathfrak{G}$ ist,

$$H^{-1}NH = H'N_1 \quad \text{mit} \quad H' \in \mathfrak{H}', N_1 \in \mathfrak{N}.$$

Erhebt man beide Seiten dieser Gleichung in die n-te Potenz, so erhält man links 1. Die n-te Potenz der rechten Seite hat, weil $\mathfrak{N}$ Normalteiler in $\mathfrak{G}_1$ ist, die Form $H'^n N_2$ mit $N_2 \in \mathfrak{N}$. Da $|\mathfrak{H}'|$ zu n teilerfremd ist, muß $H' = 1$ sein.

Damit ist Satz 1 bewiesen. Die Voraussetzung, daß $\mathfrak{R}$ ausgezeichnet ist, wurde übrigens nicht voll ausgenutzt. Es hätte genügt, von $\mathfrak{R}$ folgendes zu fordern: Mit $\mathfrak{H}^{(0)} = \mathfrak{H}, \mathfrak{H}^1, \ldots, \mathfrak{H}^{(i)}, \ldots, 1$ bezeichne man die höheren Kommutatorgruppen von $\mathfrak{H}$. Für $i = 0, 1, \ldots$, beliebige $H^{(i)} \in \mathfrak{H}^{(i)}$ und $R_\nu \in \mathfrak{R}$ sei dann

$$H^{(i)^{-1}} R_\nu H^{(i)} = H^{(i+1)} R_\mu \quad \text{mit} \quad H^{(i+1)} \in \mathfrak{H}^{(i+1)}, R_\mu \in \mathfrak{R}.$$

Wir setzen zur Abkürzung $|\mathfrak{H}| = h$ und bezeichnen mit $\mathfrak{R}^h$ den Komplex aller R^h mit $R \in \mathfrak{R}$. Aus Satz 1 erhalten wir als

Folgerung 1. *Es sei $\mathfrak{H}$ eine auflösbare Hallgruppe von $\mathfrak{G}$ mit ausgezeichnetem Repräsentantensystem $\mathfrak{R}$. Ist auch $\mathfrak{R}^h$ ein Repräsentantensystem für $\mathfrak{G}$ nach $\mathfrak{H}$, so enthält $\mathfrak{G}$ einen Normalteiler $\mathfrak{N}$ mit $\mathfrak{G} = \mathfrak{H}\mathfrak{N}$ und $\mathfrak{H} \cap \mathfrak{N} = 1$.*

Jedes Element R aus $\mathfrak{R}$ läßt sich nämlich in der Form $R = R'R''$ schreiben, wobei R' und R'' Potenzen von R sind mit $R'^h = 1, R''^n = 1$. Ist

nun auch $\mathfrak{R}'$ ein Repräsentantensystem, so ist es ebenfalls ausgezeichnet, und die Ordnungen seiner von 1 verschiedenen Elemente sind Teiler von n. Also läßt sich Satz 1 unmittelbar anwenden.

Folgerung 2. *Es sei $\mathfrak{H}$ eine auflösbare Hallgruppe von $\mathfrak{G}$ mit ausgezeichnetem Repräsentantensystem. Die von $\mathfrak{H}$ verschiedenen Durchschnitte $\mathfrak{H} \cap G^{-1}\mathfrak{H}G$ mögen im Zentrum von $\mathfrak{H}$ enthalten sein. Dann enthält $\mathfrak{G}$ einen Normalteiler $\mathfrak{N}$ mit $\mathfrak{G} = \mathfrak{H}\mathfrak{N}$ und $\mathfrak{H} \cap \mathfrak{N} = 1$.*

Wir werden wieder zeigen, daß unter den Bedingungen der Folgerung 2 ein ausgezeichnetes Repräsentantensystem existiert, das der Forderung des Satzes 1 genügt. Durch Transformation mit den Elementen aus $\mathfrak{H}$ werden die Elemente des ausgezeichneten Repräsentantensystems $\mathfrak{R}$ von $\mathfrak{G}$ nach $\mathfrak{H}$ permutiert. Wir betrachten die dabei entstehenden Transitivitätssysteme. Besteht ein solches Transitivitätssystem aus einem einzigen Element R, so ist R mit $\mathfrak{H}$ elementweise vertauschbar und besitzt daher, weil $\mathfrak{H}$ eine Hallgruppe ist, eine Ordnung, die kein Teiler von $|\mathfrak{H}|$ ist. Eine geeignete Potenz von R ist daher ein Vertreter der Nebenklasse $\mathfrak{H}R$ mit einer zu $|\mathfrak{H}|$ teilerfremden Ordnung. Sei weiter $R_1, \ldots, R_m$ ein Transitivitätssystem der Länge $m > 1$. Ist $H \in \mathfrak{H} \cap R_1^{-1}\mathfrak{H}R_1$ so wird $H = R_1^{-1}H_1R_1$ mit $H_1 \in \mathfrak{H}$ oder $R_1H = H_1R_1$. Da $\mathfrak{R}$ ausgezeichnet ist, wird bei passender Numerierung $R_1H = HR_2$, also $HR_2 = H_1R_1$. Mithin wird $H = H_1$, also H mit R_1 vertauschbar. Folglich besteht der Durchschnitt $\mathfrak{H} \cap R_1^{-1}\mathfrak{H}R_1$ genau aus den mit R_1 vertauschbaren Elementen von $\mathfrak{H}$.

Mit $\mathfrak{T}$ bezeichnen wir das Erzeugnis aller Elemente aus $\mathfrak{G}$, deren Ordnung zu $|\mathfrak{H}|$ teilerfremd ist. Man erkennt leicht, daß in jeder Nebenklasse von $\mathfrak{G}$ nach $\mathfrak{H}$ mindestens ein Element aus $\mathfrak{T}$ liegt (vgl [2], 1.3). Insbesondere sei $T_1 \in \mathfrak{T} \cap \mathfrak{H}R_1$, also $T_1 = H_1R_1$ mit $H_1 \in \mathfrak{H}$. Man ersetze R_1 durch H_1R_1 und $R_2, \ldots, R_m$ entsprechend, nämlich folgendermaßen: Ist $R_i = K_i^{-1}R_1K_i$ mit $K_i \in \mathfrak{H}$, so ersetze man R_i durch $K_i^{-1}H_1K_iR_i = H_iR_i$. Da die mit R_1 vertauschbaren Elemente voraussetzungsgemäß im Zentrum von $\mathfrak{H}$ liegen, werden die Elemente $H_1R_1, \ldots, H_mR_m$ bei Transformation mit Elementen aus $\mathfrak{H}$ nur untereinander vertauscht. Außerdem sind alle H_iR_i in $\mathfrak{T}$ enthalten.

Führt man die entsprechende Abänderung in allen Transitivitätssystemen durch, so erhält man ein ausgezeichnetes Repräsentantensystem, dessen sämtliche Elemente in $\mathfrak{T}$ enthalten sind, also ein Repräsentantensystem der in Satz 1 geforderten Art.

Satz 2. *Es sei $\mathfrak{H}$ eine auflösbare Hallgruppe in $\mathfrak{G}$ vom Index n mit ausgezeichnetem Repräsentantensystem. Hat eine der Gruppen $\mathfrak{H}', \mathfrak{H}'', \ldots$ in einer Untergruppe von $\mathfrak{G}$ den Index n, so möge sie darin ein ausgezeichnetes Repräsentantensystem besitzen. Dann enthält $\mathfrak{G}$ einen Normalteiler $\mathfrak{N}$ mit $\mathfrak{G} = \mathfrak{H}\mathfrak{N}$ und $\mathfrak{H} \cap \mathfrak{N} = 1$.*

Beweis. Mit $\mathfrak{G}_1$ bezeichnen wir wieder den Normalteiler aus allen denjenigen Elementen von $\mathfrak{G}$, die bei der Verlagerung von $\mathfrak{G}$ nach $\mathfrak{H}$ auf $\mathfrak{H}'$ abgebildet werden. Wie beim Beweis von Satz 1 schließt man wieder $\mathfrak{G} = \mathfrak{H}\mathfrak{G}_1$ und $\mathfrak{H} \cap \mathfrak{G}_1 = \mathfrak{H}'$. Weiter sei $\mathfrak{T}$ das Erzeugnis aller Elemente aus $\mathfrak{G}$, deren Ordnungen zu $|\mathfrak{H}|$ teilerfremd sind. Da in jeder Nebenklasse von $\mathfrak{G}$ nach $\mathfrak{H}$ mindestens ein Element aus $\mathfrak{T}$ liegt, wird

$$\mathfrak{G} = \sum_{\nu=1}^{n} \mathfrak{H} T_\nu \qquad (T_\nu \in \mathfrak{T}).$$

Da die T_ν bei der Verlagerung von $\mathfrak{G}$ nach $\mathfrak{H}$ auf $\mathfrak{H}'$ abgebildet werden gilt weiter

$$\mathfrak{G}_1 = \sum_{\nu=1}^{n} \mathfrak{H}' T_\nu .$$

Da somit $\mathfrak{H}'$ in $\mathfrak{G}_1$ eine Untergruppe vom Index n ist, existiert in $\mathfrak{G}_1$ ein ausgezeichnetes Repräsentantensystem für die Nebenklassen nach $\mathfrak{H}'$. Der weitere Beweis verläuft genau wie bei Satz 1.

Es ist übrigens klar, daß die Bedingungen in Satz 1, in Folgerung 1 und in Satz 2 auch notwendig sind.

Literatur

[1] R. Baer, Kriterium für die Abgeschlossenheit endlicher Gruppen, *Math. Zeitschrift*, **71** (1959), 325—334.

[2] D. G. Higman, Focal Series in Finite Groups, *Canadian J. Math.*, **5** (1953), 477—497.

[3] R. Kochendörffer, Über den Multiplikator einer Gruppe, *Math. Zeitschrift*, **63** (1956), 507—513.

[4] G. Zappa, Generalizzazione di un teorema di Kochendörffer, *Le Matematiche*, Catania, **13** (1958), 61—64.

(Eingegangen am 6. Februar 1960)

Sull'esistenza di sottogruppi normali di Hall in un gruppo finito

Di GUIDO ZAPPA in Firenze (Italia)

A L. Rédei nel suo 60° compleanno

1. Si deve a R. KOCHENDÖRFFER [1] l'introduzione del concetto di *sistema privilegiato di rappresentanti* di un sottogruppo in un gruppo. Precisamente, se G è un gruppo, e H un suo sottogruppo, dicesi sistema privilegiato di rappresentanti di H in G un insieme R di elementi di G che ha a comune con ciascun laterale di H in G uno ed un solo elemento, e tale che, comunque si prenda un elemento x in H, si abbia $x^{-1}Rx = R$.

Ovviamente, un complemento normale di H, cioè un sottogruppo normale N di G tale che $G = HN$, $H \cap N = 1$, è un sistema privilegiato di rappresentanti di H in G. Viceversa, si pone il problema di vedere quando, dati il gruppo G e il suo sottogruppo H, un sistema privilegiato di rappresentanti di H in G sia un complemento normale di H.

Limitandosi ai gruppi finiti, il caso più interessante è quello in cui H è un sottogruppo di Hall, cioè avente ordine primo con l'indice. KOCHENDÖRFFER ha dimostrato [1] che se G è un gruppo finito e H un suo sottogruppo di Sylow il cui derivato sia contenuto nel centro di H, e se esiste un sistema privilegiato di rappresentanti di H in G, esiste necessariamente un complemento normale di H.

Recentemente, in [2] ho generalizzato il precedente teorema di KOCHENDÖRFFER, sostituendo in esso, all'ipotesi che H sia un sottogruppo di Sylow a derivato contenuto nel centro, quella meno restrittiva che H sia un sottogruppo di Hall speciale (in particolare un sottogruppo di Sylow qualunque). In una osservazione fatta in fondo alla nota citata in sede di correzione delle bozze, ho indicato come l'ipotesi che H sia un sottogruppo di Hall speciale si può sostituire con l'altra, meno restrittiva, che H sia un sottogruppo di Hall disperso, vale a dire dotato di una catena principale i cui fattoriali siano tutti isomorfi a sottogruppi di Sylow di H (in particolare ciò avviene quando H è supersolubile).

Resta aperto il problema di vedere se si può sostituire all'ipotesi che H sia un sottogruppo di Hall disperso quella, ancora meno restrittiva, che esso sia soltanto risolubile. In questa Nota, pur non giungendo a tale risultato, dimostro che se esiste un sistema privilegiato di rappresentanti del sottogruppo risolubile H del gruppo finito G, esiste un complemento normale di H sotto l'ipotesi ulteriore che G e i suoi sottogruppi verifichino certe condizioni relative ai sottogruppi di Hall (cond. (a) e (b) dell'enunciato del teorema del n. 4).

2. Lemma 1. *Sia G un gruppo, H un suo sottogruppo, ed R un sistema privilegiato di rappresentanti di H in G. Allora, se r è un elemento di R, r è permutabile con ogni elemento di $H \cap r^{-1}Hr$.*

Infatti, se x è un elemento di $H \cap r^{-1}Hr$, esso è in $r^{-1}Hr$, onde esiste un elemento y di H tale che $r^{-1}yr = x$. Sarà allora $x^{-1}rx = x^{-1}r(r^{-1}yr) = x^{-1}yr$. Poichè x et y sono in H, $x^{-1}yr$ è in Hr, ed ivi è quindi $x^{-1}rx$. Ma $x^{-1}rx$ è in R, essendo R un sistema privilegiato; e poichè l'unico elemento di R che sia in Hr è r, si ha $x^{-1}rx = r$, onde r è permutabile con x, come si voleva.

Lemma 2. *Sia G un gruppo ed H un suo sottogruppo. L'insieme dei laterali di H in G venga decomposto in classi disgiunte in modo che due laterali appartengano alla stessa classe quando e solo quando sono trasformati l'uno nell'altro da un elemento di H. Allora, scelto un laterale L_i per ciascuna classe C_i, se in ciascun laterale scelto L_i c'è un elemento r_i che sia permutabile con ogni elemento di $H \cap r_i^{-1}Hr_i$, l'insieme R dei trasformati degli elementi r_i mediante gli elementi di H è un sistema privilegiato di rappresentanti di H in G.*

E' evidente che ogni laterale di H in G ha almeno un elemento in R, e che, se x è in H, $x^{-1}Rx = R$. Per provare che R è un sistema privilegiato di rappresentanti di H in G basterà far vedere che se due elementi di R appartengono allo stesso laterale di H, essi coincidono.

Siano $x^{-1}r_ix$, $y^{-1}r_jy$ due elementi di R appartenenti allo stesso laterale di H (r_i, r_j in R; x, y in H). Dovrà aversi anzitutto $r_i = r_j$, altrimenti $x^{-1}r_ix$ e $y^{-1}r_jy$ apparterrebbero addirittura a due laterali contenuti in classi distinte. Si avrà $x^{-1}r_ix = hy^{-1}r_iy$ con h conveniente elemento di H. Ne discende

$$r_i^{-1}yh^{-1}x^{-1}r_i = yx^{-1}. \tag{1}$$

Orbene, essendo $yh^{-1}x^{-1}$ in H, si ha che $r_i^{-1}yh^{-1}xr_i$, cioè yx^{-1}, è in $r_i^{-1}Hr_i$. D'altra parte yx^{-1} è pure in H, onde yx^{-1} è in $H \cap r_i^{-1}Hr_i$. Per ipotesi è allora $r_i^{-1}yx^{-1}r_i = yx^{-1}$. Dalla (1) quindi segue $yh^{-1}x^{-1} = yx^{-1}$, cioé $h = 1$, onde $x^{-1}r_ix = y^{-1}r_iy$, come si voleva.

3. Sia π un insieme di numeri primi, e π' l'insieme complementare di π rispetto all'insieme di tutti i numeri primi.

Diremo *π-intero* ogni intero positivo i cui fattori primi appartengano tutti a π. Diremo *π-gruppo* (*π-elemento*) un gruppo finito (un elemento di un gruppo finito) il cui ordine sia un π-intero, e *π-sottogruppo* di un gruppo G un sottogruppo di G che sia un π-gruppo. Diremo poi *π-sottogruppo di Hall* di un gruppo finito G un π-sottogruppo di G il cui ordine sia il massimo π-intero che divida l'ordine di G.

Si dirà che un gruppo finito G verifica la *π-condizione esistenziale di Hall* se esso contiene un π-sottogruppo di Hall, e si dirà che G verifica la *π-condizione d'immersione di Hall* se esso verifica la π-condizione esistenziale di Hall e, detti H un π-sottogruppo di Hall e D un π-sottogruppo di G, si ha che D è contenuto in un coniugato ad H in G.

Proviamo anzitutto il seguente:

Lemma 3. *Se un gruppo finito G verifica la π-condizione d'immersione di Hall, la verifica anche ogni sottogruppo normale di G il cui indice sia un π-intero.*

Sia hk l'ordine di G, con h π-intero e k π'-intero. Sia poi N un sottogruppo normale di G, il cui indice sia un π-intero, e sia H un π-sottogruppo di Hall di G. L'ordine di H vale h, mentre l'ordine di N è multiplo di k, onde l'ordine di $H \cup N$ è divisibile per hk, vale a dire $H \cup N = G$. Si ha poi $H \cup N = HN$, essendo N normale in G, onde, detto $o(X)$ l'ordine di un gruppo X, si ha

$$o(H \cap N) = \frac{o(H)o(N)}{o(G)} = \frac{o(N)}{k}.$$

Poichè k è il massimo π'-intero che divide l'ordine di N, si ha che l'ordine di $H \cap N$ è il massimo π-intero che divide l'ordine di N, onde $H \cap N$ è un π-sottogruppo di Hall di N, vale a dire N verifica la π-condizione esistenziale di Hall.

Si noti ora che, se L è un π-sottogruppo di Hall di N, L è contenuto in un coniugato $\bar{H}$ di H (perchè G verifica la π-condizione di immersione di Hall) onde si ha $L \subseteq N \cap \bar{H}$, e poichè $N \cap \bar{H}$ è di Hall per N, si ha $L = N \cap \bar{H}$. Essendo $\bar{H}$ un π-sottogruppo di Hall di G, al pari di H, ne segue che i π-sottogruppi di Hall di N sono dati tutti e soli dalle intersezioni di N coi π-sottogruppi di Hall di G.

Sia ora D un π-sottogruppo di N, e L^* un π-sottogruppo di Hall di N. Per quanto si è osservato, è $L^* = N \cap H^*$, con H^* π-sottogruppo di Hall di G. Inoltre D è contenuto in un coniugato H_0 di H^* in G, quindi anche in

$N \cap H_0$. Sia c un elemento di G tale che $c^{-1}H^*c = H_0$. Ogni elemento di H^*c trasforma H^* in H_0, e poichè in H^*c c'è almeno un elemento di N, esiste un elemento b di N tale che $b^{-1}H^*b = H_0$, cioè tale che $b^{-1}L^*b = b^{-1}(N \cap H^*)b = N \cap H_0$. Poichè $N \supseteq D$ e $H_0 \supseteq D$, si ha $b^{-1}L^*b \supseteq D$, onde, essendo D un π-sottogruppo di N e L^* un π-sottogruppo di Hall di N, si ha che N verifica la π-condizione d'immersione di Hall.

4. Possiamo ora provare il

Teorema. *Sia G un gruppo finito tale che:*

(*a*) *G verifica la π-condizione d'immersione di Hall;*

(*b*) *Ogni sottogruppo di G verifica la π-condizione esistenziale di Hall, e la π'-condizione esistenziale di Hall;*

(*c*) *Esiste un π-sottogruppo di Hall risolubile H di G, dotato di un sistema privilegiato R di rappresentanti.*

Allora G possiede un π'-sottogruppo di Hall normale.

Procediamo per induzione rispetto all'ordine del gruppo. Si decomponga anzitutto G in laterali di H prendendo gli elementi di R come rappresentanti dei laterali. Si esegua poi il traslato (Verlagerung) del gruppo G rispetto ad H. Sia g un elemento di H non contenuto in H', e sia r un elemento di R. Si avrà $rg = g(g^{-1}rg) = g\bar{r}$, con $\bar{r}$ ancora elemento di R, onde, indicato con $V(x)$ il traslato dell'elemento x di G, e con k il massimo π'-intero che divide l'ordine di G, si ha che i laterali di H in G sono in numero di k, e pertanto $V(g) = H'g^k$. Poichè k è primo con l'ordine di H, quindi anche con l'ordine di g, esiste un intero $d > 0$ tale che $(g^k)^d = 1$, onde $V(g^d) = H'g$. Ciò basta per concludere che $V(G) = H/H'$, onde G è omomorfo sopra H/H', e il nucleo di tale omomorfismo è un sottogruppo M normale in G, tale che G/M sia isomorfo ad H/H'. Evidentemente è $H' = H \cap M$. Essendo H risolubile, è $H' \subset H$, onde $M \subset G$.

Ogni π'-elemento di G è in M, perchè ad esso corrisponde l'unità nel suddetto omomorfismo di G sul π-gruppo H/H'. Mostriamo ora che esiste un sistema privilegiato di rappresentanti di H in G formato unicamente da π'-elementi, cioè contenuto in M.

Il sistema R è formato di classi complete di elementi coniugati rispetto ad H. Sia K_i la generica di queste classi, e sia r_i un elemento scelto in K_i. Si abbia $r_i^{-1}Hr_i = \bar{H}$. Allora, se x è in $H \cap \bar{H}$ si ha, in base al lemma 1, $r_i^{-1}xr_i = x$. Di conseguenza r_i è nel centralizzante C di $H \cap \bar{H} = L$.

Sia ora $B = C \cap H$. Mostriamo che B è un π-sottogruppo di Hall di C. Per la (*b*) dell'enunciato del teorema, C possiede π-sottogruppi di Hall: sia B^* uno di essi. Si noti che $B^* \supseteq L$, perchè, essendo L un π-sottogruppo normale di C, LB^* è anch'esso un π-sottogruppo di C, onde $B^* \supseteq LB^* \supseteq L$. Per

la (a) dell'enunciato del teorema, B^* deve essere contenuto in un coniugato H^* di H. Si avrà allora $L \subseteq B^* \subseteq H^*$, ed essendo B^* un π-sottogruppo di Hall di C, è $B^* = C \cap H^*$. Detto y un elemento di G tale che $y^{-1}Hy = H^*$, si ha che ogni elemento del laterale Hy trasforma H in H^*. Se r è l'elemento di R che rappresenta detto laterale, si avrà $r^{-1}Hr = H^*$. Per il lemma 1, r è permutabile con ogni elemento di $H^* \cap H$, e poichè $L \subseteq H$, $L \subseteq B^* \subseteq H^*$, e quindi $L \subseteq H \cap H^*$, r è permutabile con ogni elemento di L, vale a dire è in C. Si avrà allora $r^{-1}Br = r^{-1}(C \cap H)r = (r^{-1}Cr) \cap (r^{-1}Hr) = C \cap H^* = B^*$, ed essendo B^* un π-sottogruppo di Hall di C, tale è B, come si era affermato.

Per la (b) dell'enunciato del teorema, C possiede un π'-sottogruppo di Hall D. Si avrà allora $C = BD$. Poichè r_i è in C, si avrà $r_i = b_i d_i$, con b_i in B, e d_i in D. Essendo $B \subseteq H$, r_i e d_i appartengono allo stesso laterale di H.

Nel laterale Hr_i, che abbiamo scelto nella classe K_i, prendiamo allora come rappresentante l'elemento d_i, anzichè l'elemento r_i. Si avrà $d_i^{-1}Hd_i = r_i^{-1}b_i^{-1}Hb_i r_i = r_i^{-1}Hr_i$, onde $H \cap d_i^{-1}Hd_i = L$. Essendo d_i in C, d_i è permutabile con ogni elemento di L. Allora, per il lemma 2, si ha che i trasformati, mediante gli elementi di H, degli elementi d_i scelti nei laterali Hr_i presi uno da ciascuna classe K_i formano un sistema privilegiato di rappresentanti $\bar{R}$ di H in G. Ma gli elementi d_i, e quindi anche i loro trasformati, sono π'-elementi, e quindi sono contenuti in M. Essendo ogni laterale di B in M contenuto in uno ed un solo laterale di H in G, si ha che $\bar{R}$ è anche un sistema privilegiato di rappresentanti di B in M, poichè si ha $x^{-1}\bar{R}x = \bar{R}$ per x in H e quindi in particolare per x in B. Inoltre, per il lemma 3, che può applicarsi perchè in G vale la (a), M verifica la π-condizione di immersione di Hall, ed ovviamente ogni suo sottogruppo, quale sottogruppo di G, verifica, per la (b) la π-condizione esistenziale e la π'-condizione esistenziale di Hall. In base all'ipotesi d'induzione, allora, M ha un π'-sottogruppo di Hall normale N. Esso è caratteristico in M, quindi è un π'-sottogruppo di Hall normale in G.

Il teorema è quindi dimostrato.

Bibliografia

[1] R. Kochendörffer, Ein Satz über Sylowgruppen, *Mat. Nachrichten*, **17** (1959), 189—194.
[2] G. Zappa, Generalizzazione di un teorema di Kochendörffer, *Le Mathematiche*, Catania, **13** (1958), 61—64.

(Ricevuto l'11 febbraio 1960)

A prime decomposition symbol for certain non Abelian number fields

By A. FRÖHLICH in London

Dedicated to Professor L. Rédei on his 60th birthday

In a recent paper (cf. [4])[1]) I gave a rational description of normal[2]) fields A of prime power degree l^{n+1} which contain an Abelian subfield K of degree l^n. This made it possible in particular to determine in purely rational terms the group extensions of a group of order l by the Galois group of K which are realised by such fields A, and the relative ramification types of A/K which will occur.

In the present paper we shall consider normal non cyclic fields A of degree 8. Every such field will contain a biquadratic field[3]) $P(\sqrt{d_1}, \sqrt{d_2})$ and so the theory of [4] can be applied. We shall principally be concerned with a new symbol $[a_1, a_2, a]_c$; the variable c is a factor system class of the "Vierer-gruppe" in the group of square roots of unity, and the variables a_1, a_2, a are non zero rational numbers satisfying certain conditions. In the significant cases a_1, a_2 coincide with the independent quadratic discriminants d_1, d_2. When a is then a rational prime which is total norm residue of $P(\sqrt{d_1}, \sqrt{d_2})$, the value of the symbol will determine the decomposition of (a) in a field A, belonging to the factor system class c. Though we are of course principally interested in non Abelian fields, it will be useful for a proper theoretical understanding to treat simultaneously all fields containing $P(\sqrt{d_1}, \sqrt{d_2})$. In order to keep this paper at a reasonable length we shall however make at some stage (cf. (2.15)) the restriction that d_1, d_2 be odd.

It will be seen that the symbol $[a_1, a_2, a]_c$ is unrestrictedly multiplicative in a and c, and partially multiplicative in a_1, a_2. It moreover admits two basic inversion laws. For the first of these we shall interpret the symmetric

---

[1]) Numbers in square brackets refer to the literature list.

[2]) Terms such as "normal", "Abelian", "degree" are to be understood in the absolute sense, i. e. with respect to the rational field, unless otherwise qualified.

[3]) P is the rational field.

group of permutations on three symbols simultaneously as group of permutations of the three quadratic discriminants associated with the field $P(\sqrt{d_1}, \sqrt{d_2})$ and as a group of automorphisms of the "Vierer-gruppe". Each permutation then gives rise to an inversion formula. The second inversion law on the other hand is closely connected with quadratic reciprocity in quadratic fields.

We shall also give explicit expressions for the new symbol in terms of values of rational residue characters associated with certain rational ternary quadratic forms, and thus obtain rational prime-decomposition criteria for a class of non Abelian fields. Some of the multiplication laws and inversion formulae will then have interesting interpretations in terms of the explicit expressions given.

Decomposition criteria for certain non Abelian fields of degree 8 [4]) were found for the first time by S. KURODA (cf. [7]), whose results where subsequently extended by FURUTA to the relative case (cf. [5], [6]). The class of fields covered by S. KURODA was discussed again in a paper of the author's (cf. [3]), in conjunction with a general theory of the restricted biquadratic residue symbol. In view of our present restriction to odd quadratic discriminants there is no overlap between the class of fields considered here and that considered in the quoted papers. The results of [3] can however easily be rephrased in terms of suitable symbols $[a_1, a_2, a]_c$.

Our symbol has a "restricted" argument domain. It was L. RÉDEI who first saw the importance of such restricted symbols when dealing with problems of a "non-Abelian" nature (cf. [10], [11]). Altogether our subject matter is closely related to L. RÉDEI's work on quadratic fields (cf. [8], [9], [11]), and in particular to the symbol defined by him in [9], and applied to a number of problems. L. RÉDEI's symbol is in fact essentially the same as ours for a certain fixed value of the variable c, and the multiplication and inversion laws for this case can already be found in his original paper.

§ 1.

P is throughout the rational field. The Galois group of a normal extension $\mathcal{A}$ of an algebraic number field K will be denoted by $\Gamma(\mathcal{A}/K)$. We shall use the results of class field theory in a finite number field K as formulated in terms of idèle class characters (cf. [1]), i.e. of continuous characters of the idèle group of K which take trivial value on the principal idèles. To each Abelian extension $\mathcal{A}/K$ there will then correspond a group $\Phi(\mathcal{A}/K)$ of such characters; $\Phi(\mathcal{A}/K)$ can also be considered as the group of

[4]) And of course for composites of such fields with Abelian fields.

continuous characters of $\Gamma(\mathcal{A}/K)$. If φ is an idèle class character in K we denote by K_φ the associated class field; thus $\Phi(K_\varphi/K)$ is a cyclic group with generator φ.

If Ω is a subfield of K we can associate with every idèle class character ψ in Ω, a character[5]) $R_{K/\Omega}\psi$ in K by the rule (cf. [4])

$$R_{K/\Omega}\psi(\mathfrak{m}) = \psi(N_{K/\Omega}\mathfrak{m}) \tag{1.1}$$

for all idèles $\mathfrak{m}$ in K, $N_{K/\Omega}$ being the norm mapping. $R_{K/\Omega}$ is a homomorphism.

Denote by Q_φ the group of ideals in K which are integral for and prime to the conductor[6]) $\mathfrak{f}(\varphi)$ of the character φ in K. For $\mathfrak{a} \in Q_\varphi$ choose any idèle $\mathfrak{m}$ with contents $(\mathfrak{m}) = \mathfrak{a}$, whose components $\mathfrak{m}_\mathfrak{p}$ have value 1 whenever $\mathfrak{p}$ divides $\mathfrak{f}(\varphi)$ or is an infinite prime. $\varphi(\mathfrak{m})$ is then independent of the particular choice of $\mathfrak{m}$ within the stated conditions so that we may write

$$\varphi(\mathfrak{m}) = \theta_\varphi(\mathfrak{a}). \tag{1.2}$$

θ_φ is a character of the ideal group Q_φ; $\theta_\varphi(\mathfrak{a}) = 1$ if and only if we have for the Artin symbol of $\mathfrak{a}$, $(K_\varphi/K;\mathfrak{a}) = 1$. For characters φ_1, φ_2 we get

$$\theta_{\varphi_1\varphi_2}(\mathfrak{a}) = \theta_{\varphi_1}(\mathfrak{a})\theta_{\varphi_2}(\mathfrak{a}) \tag{1.3}$$

whenever $\mathfrak{a} \in Q_{\varphi_1} \cap Q_{\varphi_2}$.

Let Q_φ^* be the group of non zero elements α of K with $(\alpha) \in Q_\varphi$. We write for $\alpha \in Q_\varphi^*$

$$\chi_\varphi(\alpha) = \Pi\varphi_\mathfrak{p}(\alpha) \tag{1.4}$$

the product extending over the finite prime divisors ramified at φ. χ_φ is a residue character, and again

$$\chi_{\varphi_1\varphi_2}(\alpha) = \chi_{\varphi_1}(\alpha)\chi_{\varphi_2}(\alpha) \tag{1.5}$$

for $\alpha \in Q_{\varphi_1}^* \cap Q_{\varphi_2}^*$. As $\varphi(\alpha) = 1$ we also get

$$\theta_\varphi((\alpha)) = \chi_\varphi^{-1}(\alpha)\varphi_\infty(\alpha) \tag{1.6}$$

where φ_∞ is the product of the infinite components of φ.

Assume now K to be normal over a subfield Ω. An ideal $\mathfrak{A}$ in K is said to be *primitive* (with respect to Ω) if in its prime power decomposition

$$\mathfrak{A} = \prod_i \mathfrak{P}_i^{r_i}$$

---

[5]) The term "character" without further qualification will be used as synonymous with "idèle class character".

[6]) $\mathfrak{f}(\varphi)$ is considered as an ideal, i.e. the prime divisors of $\mathfrak{f}(\varphi)$ are the finite ramified prime divisors (prime ideals).

no two of the prime ideals $\mathfrak{P}_i$ occurring non trivially are conjugate over Ω. Let φ be a character in K such that K_φ is a *central extension* of K over Ω, i.e. that K_φ is normal over Ω and $\Gamma(K_\varphi/K)$ lies in the centre of $\Gamma(K_\varphi/\Omega)$. Such a character φ is characterised by the equations

$$\varphi^\gamma = \varphi \quad \text{for all} \quad \gamma \in \Gamma(K/\Omega). \tag{1.7}$$

Let $N(K/\Omega)$ be the group of ideals in Ω which are norms of ideals in K. Every ideal $\mathfrak{a}$ in $N(K/\Omega)$ is then also the norm of a primitive ideal $\mathfrak{A}$ in K; if $\mathfrak{a}$ is integral for and prime to the conductor $\mathfrak{f}(\varphi)$ then so is $\mathfrak{A}$. Hence $\theta_\varphi(\mathfrak{A})$ is defined; in view of (1.7) its value will not depend on $\mathfrak{A}$ but solely on $\mathfrak{a}$. We may thus write

$$\theta_\varphi(\mathfrak{A}) = (N_{K/\Omega}\theta_\varphi)(\mathfrak{a}). \tag{1.8}$$

If $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are ideals in $N(K/\Omega)$ then they are norms of primitive ideals $\mathfrak{A}_1$ and $\mathfrak{A}_2$ so that $\mathfrak{A}_1\mathfrak{A}_2$ is again primitive. Hence

$$(N_{K/\Omega}\theta_\varphi)(\mathfrak{a}_1\mathfrak{a}_2) = (N_{K/\Omega}\theta_\varphi)(\mathfrak{a}_1)\cdot(N_{K/\Omega}\theta_\varphi)(\mathfrak{a}_2). \tag{1.9}$$

On the other hand we have by (1.3)

$$(N_{K/\Omega}\theta_{\varphi_1\varphi_2})(\mathfrak{a}) = (N_{K/\Omega}\theta_{\varphi_1})(\mathfrak{a})\cdot(N_{K/\Omega}\theta_{\varphi_2})(\mathfrak{a}). \tag{1.10}$$

Both in (1.9) and in (1.10) the left hand side is defined provided that the right hand side is.

§ 2.

Throughout Γ is a fixed, non cyclic group of order 4 with γ_1, γ_2 as a given, ordered pair of generators. F is the group of factor system classes of Γ in the group E of square roots of unity. For any factor system $\bar{c}$ in a given class c the elements

$$\begin{cases} \bar{c}(\gamma_i, 1)\,\bar{c}(\gamma_i, \gamma_i) = (-1)^{c(\gamma_i)} \\ \bar{c}(\gamma_1, \gamma_2)\,\bar{c}(\gamma_2, \gamma_1)^{-1} = (-1)^{c(\gamma_1, \gamma_2)} \end{cases} \qquad (i = 1, 2) \tag{2.1}$$

depend only on c and will in turn determine c uniquely. Accordingly we represent the elements of F as sequences

$$c = [c(\gamma_1), c(\gamma_2), c(\gamma_1, \gamma_2)] \tag{2.2}$$

of integers mod 2, multiplication in F being given by component-wise addition mod 2. Each such sequence will in fact represent an element of F. It will be useful to write

$$\gamma_1\gamma_2 = \gamma_3, \quad c(\gamma_3) \equiv c(\gamma_1) + c(\gamma_2) + c(\gamma_1, \gamma_2) \pmod 2. \tag{2.3}$$

We shall find it convenient to consider the $c(\gamma_i)$, and $c(\gamma_1, \gamma_2)$ actually as integers, normalised to the values 0 or 1.

Let d_1, d_2 be an ordered pair of independent quadratic discriminants. Then

$$\mathsf{K} = \mathsf{P}(\sqrt{d_1}, \sqrt{d_2}) \tag{2.4}$$

is a non cyclic, biquadratic field. We shall repeatedly use the symbols

$$\left\{\begin{array}{l} d_3 = d_1 d_2/(d_1, d_2)^2, \\ f_1 = (d_2, d_3), \quad f_2 = (d_3, d_1), \quad f_3 = (d_1, d_2), \end{array}\right. \tag{2.5}$$

where (a, b) is always taken to be positive. With the given pair d_1, d_2 we associate the isomorphism

$$g_{d_1, d_2} = g: \quad \Gamma \cong \Gamma(\mathsf{K}/\mathsf{P})$$

uniquely determined by

$$\sqrt{d_i}^{g(\gamma_j)-1} = (-1)^{\delta_{ij}} \qquad (i, j = 1, 2), \tag{2.6}$$

δ_{ij} being the Kronecker symbol.

Let Σ be the symmetric group of permutations on the symbols 1, 2, 3. For each $\pi \in \Sigma$ we have then $\mathsf{K} = \mathsf{P}(\sqrt{d_{\pi(1)}}, \sqrt{d_{\pi(2)}})$ and there exists a unique isomorphism

$$g_\pi: \quad \Gamma \cong \Gamma(\mathsf{K}/\mathsf{P})$$

such that

$$\sqrt{d}_{\pi(i)}^{g_\pi(\gamma_j)-1} = (-1)^{\delta_{ij}} \qquad (i, j = 1, 2). \tag{2.7}$$

There will then exist a unique automorphism π' of Γ such that

$$g_\pi = g \circ \pi'. \tag{2.8}$$

The characters φ in K with

$$\varphi^2 = 1 = \varphi^{\gamma-1} \tag{2.9}$$

for all $\gamma \in \Gamma(\mathsf{K}/\mathsf{P})$ form a group which we shall here denote by Φ_K. The fields K_φ $(\varphi \in \Phi_\mathsf{K})$ are precisely those cyclic extensions of K of relative degree 2 (or 1) which are central extensions of K over P, i. e. which are (absolutely) normal. For each φ $\Gamma(\mathsf{K}_\varphi/\mathsf{P})$ is a group extension of $\Gamma(\mathsf{K}_\varphi/\mathsf{K})$ by $\Gamma(\mathsf{K}/\mathsf{P})$ and thus determines a class b_φ in the group $F(\mathsf{K}, \varphi)$ of factor system classes of $\Gamma(\mathsf{K}/\mathsf{P})$ in $\Gamma(\mathsf{K}_\varphi/\mathsf{K})$. To describe this extension in terms of the fixed group F we only have to note that the isomorphism $g: \Gamma \cong \Gamma(\mathsf{K}/\mathsf{P})$ together with the homomorphism $\varphi: \Gamma(\mathsf{K}_\varphi/\mathsf{K}) \to E$ gives rise to a homomorphism

$$g^*: \quad F(\mathsf{K}, \varphi) \to F. \tag{2.10}$$

If $\varphi \neq 1$, then φ is an isomorphism, and so g^* is an isomorphism. On replacing g by g_π we get

$$g_\pi^* = \pi^* \circ g^* \tag{2.11}$$

where π^* is the automorphism of F induced by π'.

For fixed d_1, d_2 we shall write

$$g^*(b_\varphi) = c_\varphi . \tag{2.12}$$

Explicitly we have for $c = c_\varphi$, for any representatives $\bar{\gamma}_i$ of $g(\gamma_i)$ in $\Gamma(\mathsf{K}_\varphi/\mathsf{P})$ $(i = 1, 2)$, and for ω as generator of $\Gamma(\mathsf{K}_\varphi/\mathsf{K})$ the relations [7])

$$\bar{\gamma}_i^2 = \omega^{c(\gamma_i)} \quad (i = 1, 2), \quad (\bar{\gamma}_1, \bar{\gamma}_2) = \omega^{c(\gamma_1, \gamma_2)}. \tag{2.13}$$

Thus K_φ is non Abelian if and only if $c(\gamma_1, \gamma_2) = 1$.

The c_φ are those classes in F which in terms of the given isomorphism g are *realised arithmetically* by actual extensions of K. By [4] (Theorem 1) we have

Theorem 1. *$\varphi \to c_\varphi$ is a homomorphism whose kernel is the group of characters $R_{\mathsf{K}/\mathsf{P}}\psi$ with $\psi^2 = 1$.*

The classes c_φ will thus form a subgroup $A(d_1, d_2)$ of F. As a special case of the general criterion in [4] (Theorem 7) we get

Theorem 2. *An element c in F will lie in $A(d_1, d_2)$ if and only if*

$$\left(\frac{-1, d_1}{p}\right)^{c(\gamma_1)} \left(\frac{-1, d_2}{p}\right)^{c(\gamma_2)} \left(\frac{d_1, d_2}{p}\right)^{c(\gamma_1, \gamma_2)} = 1$$

for all rational prime divisors p.

It will of course always suffice to consider only the prime factors p of d_1, d_2.

Those characters φ in Φ_K whose conductor $\mathfrak{f}(\varphi)$ contains only such prime ideals which are also contained in $d_1 d_2$ form a subgroup Φ_K^* of $\Phi_\mathsf{K} \cdot \mathfrak{f}(\varphi)$ is always the relative discriminant of $\mathsf{K}_\varphi/\mathsf{K}$. The element φ of Φ_K^* are thus characterised in Φ_K by the property that every rational discriminant prime divisor of K_φ is already a discriminant prime divisor of K. The importance of the group Φ_K^* was exhibited in Theorems 5 (Corollary 1) and 11 in [4].

Let K^* be the genus field of K (in the narrow sense) i.e. the maximal (absolutely) Abelian field which contains K and has relative discriminant (1) over K. $\Phi(\mathsf{K}^*/\mathsf{K})$ is then the subgroup of Φ_K^* of those characters satisfying the equations

$$\chi_\varphi = 1, \quad c_\varphi = 1. \tag{2.14}$$

[7]) In (2.13) $(\bar{\gamma}_1, \bar{\gamma}_2)$ is the commutator.

From now on, and for the remainder of this paper it will be assumed that

$$d_1 \equiv d_2 \equiv 1 \pmod 4. \tag{2.15}$$

Then we have (cf. [4], Theorems 8, 11):

Theorem 3. *For each* $c \in A(d_1, d_2)$ $\exists \varphi \in \Phi_K^*$ *with* $c = c_\varphi$, *and the characters* $\varphi \in \Phi_K^*$ *with this property form a coset* $\Phi^*(c) = \Phi^*(d_1, d_2, c)$ *of*[8] $\Phi_K^* \bmod \Phi(K^*/K)$.

From the last assertion it follows that for each $c \in A(d_1, d_2)$ we have a unique residue character

$$\chi_c = \chi_\varphi \qquad (\varphi \in \Phi^*(d_1, d_2, c)), \tag{2.16}$$

and so a unique conductor

$$\mathfrak{d}_c = \mathfrak{f}(\varphi). \tag{2.17}$$

$\mathfrak{d}_c$ is the relative discriminant over K of all fields K_φ with $\varphi \in \Phi^*(c)$.

For an explicit description of χ_c we note firstly that in view of (2.9) conjugate prime ideals in K have the same ramification behaviour in K_φ. In the second place as "even" prime ideals can be neglected the only possible non trivial prime components of χ_c are those given by the quadratic residue symbols $\left(\frac{\cdot}{\mathfrak{P}}\right)$. It will thus suffice to find those rational prime factors of $d_1 d_2$ which are coprime to $\mathfrak{d}_c$. Every rational prime factor p of $d_1 d_2$ divides one and only one of the integers f_i defined in (2.5). Assume, say $p \mid f_1$. Then the inertia group of p in K/P is generated by $g(\gamma_2)$, and so by (2.13) $\omega^{e(\gamma_2)}$ will generate the inertia group in K_φ/K of the prime divisors of p in K. In this manner we have proved the

Proposition 2.1. $(p, \mathfrak{d}_c) = 1$ *if and only if*

$$(p, f_1^{e(\gamma_2)} f_2^{e(\gamma_1)} f_3^{e(\gamma_3)}) = 1.$$

Next we consider criteria for K_φ to be real, assuming now that K is real. If first $\left(\frac{-1, d_i}{p}\right) = -1$ for some i and some p, then K^* is imaginary. It follows easily from Theorem 3 that there will be both real and imaginary fields K_φ with $\varphi \in \Phi^*(c)$.

Now assume that $\left(\frac{-1, d_i}{p}\right) = 1$ for all p and for $i = 1, 2$. In this case the restricted biquadratic residue symbols $\left[\frac{-1}{d_i}\right]$, $\left[\frac{-1}{f_i}\right]$ are defined (cf. [3]),

[8] $\Phi^*(c)$ will actually depend on the ordered pair d_1, d_2. Whenever this is to be stressed the symbol $\Phi^*(d_1, d_2, c)$ will be used.

and the criterion of Theorem 2 reduces to

$$\left(\frac{d_1, d_2}{p}\right)^{c(\gamma_1, \gamma_2)} = 1.$$

Thus if $c(\gamma_1, \gamma_2) = 1$ then for $p | f_i$ we have $\left(\frac{p}{d_i}\right) = 1$; therefore the symbols $\left[\frac{f_i}{d_i}\right]$ are defined. We then have

Theorem 4. *Assume d_1, d_2 to be products of primes $\equiv 1 \pmod 4$, and that $c \in A(d_1, d_2)$. The property of $K_\varphi(\varphi \in \mathfrak{D}^*(c))$ to be real or imaginary will then solely depend on c.*

For $c(\gamma_1, \gamma_2) = 0$, K_φ is real if and only if

$$\left[\frac{-1}{d_1}\right]^{c(\gamma_1)} \left[\frac{-1}{d_2}\right]^{c(\gamma_2)} = 1.$$

For $c(\gamma_1, \gamma_2) = 1$, K_φ is real if and only if

$$\left[\frac{-1}{d_1}\right]^{c(\gamma_1)} \left[\frac{-1}{d_2}\right]^{c(\gamma_2)} \left[\frac{f_1}{d_1}\right] \left[\frac{f_2}{d_2}\right] \left[\frac{f_3}{d_3}\right] \left[\frac{-1}{f_3}\right] \left(\frac{f_2}{f_3}\right) = 1.$$

We shall not give a proof of this theorem. Such a proof would follow the line of argument in [2] p. 248—249. For $(d_1, d_2) = 1$, $c(\gamma_1) = c(\gamma_2) = 0$, $c(\gamma_1, \gamma_2) = 1$ the criterion is effectively due to L. RÉDEI (cf. [8]).

There is an apparent asymmetry in the factor $\left(\frac{f_2}{f_3}\right)$ occurring in the last formula of the theorem. The hypothesis however implies that $\left(\frac{f_2}{f_3}\right) = \left(\frac{f_1}{f_3}\right)$, and in fact more generally that $\left(\frac{f_2}{f_3}\right) = \left(\frac{f_i}{f_j}\right)$ for all $i, j = 1, 2, 3$; $i \neq j$.

§ 3.

We consider triplets

$$\{d_1, d_2, c\}$$

where d_1, d_2 *are square free integers* $\equiv 1 \pmod 4$ with $d_i = 1$ as possible values and where $c \in F$. The following postulates are to be satisfied:

A. (i) *Whenever d_1, d_2 are independent quadratic discriminants* (i. e. $1 \neq d_1 \neq d_2 \neq 1$) *then $c \in A(d_1, d_2)$,* i. e. *for all p*

$$\left(\frac{-1, d_1}{p}\right)^{c(\gamma_1)} \left(\frac{-1, d_2}{p}\right)^{c(\gamma_2)} \left(\frac{d_1, d_2}{p}\right)^{c(\gamma_1, \gamma_2)} = 1.$$

(ii) *Whenever* $d_1 = d_2$ *then for all* p

$$\left(\frac{-1, d_2}{p}\right)^{c(\gamma_2)+c(\gamma_1,\gamma_2)} = 1.$$

A triplet $\{d_1, d_2, c\}$ with d_1, d_2 independent quadratic discriminants will be called *non-degenerate*. The degenerate triplets are thus those for which $d_i = 1$ for some i or $d_1 = d_2$. In the non degenerate case we shall for fixed d_1, d_2 adopt the notation of § 2.

With each triplet $\{d_1, d_2, c\}$ we associate a multiplicative group $S\{d_1, d_2, c\}$ of non zero rational numbers. We consider separately three cases (i) $\{d_1, d_2, c\}$ is non degenerate; (ii) $\{d_1, d_2, c\}$ is degenerate, $d_1 = d_2 \neq 1$ and $c(\gamma_2) + c(\gamma_1, \gamma_2) \equiv 1 \pmod 2$; (iii) $\{d_1, d_2, c\}$ is degenerate but the other conditions in (ii) are not both satisfied. In all cases $S\{d_1, d_2, c\}$ is generated by its integral elements. It will therefore suffice to give the conditions for an integer a to lie in this group.

B. *Case* (i):

$$\left(\frac{a, d_i}{p}\right) = 1 \text{ for } i = 1, 2 \text{ and for all } p, \quad (a, f_1^{c(\gamma_2)} f_2^{c(\gamma_1)} f_3^{c(\gamma_3)}) = 1,$$

also $a > 0$ *whenever* $d_1 d_2$ *has a prime divisor* $p \equiv 3 \pmod 4$.

Case (ii):

$$\left(\frac{a, d_1}{p}\right) = 1 \text{ for all } p, \ (a, d_1) = 1.$$

Case (iii): a *always lies in* $S\{d_1, d_2, c\}$.

The defining condition in case (i) apart from the sign condition can be restated in the form

B'. (a) *is prime to the relative discriminant* $\mathfrak{d}_c$. *Also* (a) *is norm of some ideal* $\mathfrak{A}$ *in* K, *and for every such* $\mathfrak{A}$, $(K^*/K; \mathfrak{A}) = 1$.

For every triplet $\{d_1, d_2, c\}$ and for all $a \in S(d_1, d_2, c)$ we now define the symbol

$$[d_1, d_2, a]_c$$

as follows. In case (iii)

$$[d_1, d_2, a]_c = 1. \tag{3.1}$$

In case (ii)

$$[d_1, d_2, a]_c = \left[\frac{a}{d_1}\right]\left[\frac{-1}{d_1}\right]^{(\operatorname{sign} a - 1)/2} \tag{3.2}$$

where we note that by **B** the restricted biquadratic residue symbols $\left[\frac{a}{d_1}\right]$, $\left[\frac{-1}{d_1}\right]$ are defined (cf. [3]).

In the non degenerate case (a) will be ideal norm of K. Also we see that the ideal (a) is integral for and prime to $\mathfrak{d}_c$ so that the symbol $(N_{\mathsf{K}/\mathsf{P}}\,\theta_\varphi)\,(a))$ (cf. § 1. (1.8)) is defined for all $\varphi \in \Phi^*(d_1, d_2, c)$. Let $\mathfrak{A}$ be a primitive ideal in K with norm (a). By $\mathbf{B}'$ $(\mathsf{K}^*/\mathsf{K}; \mathfrak{A}) = 1$. If $\varphi, \varphi_1 \in \Phi^*(d_1, d_2, c)$ then $\varphi_1\varphi^{-1} \in \Phi(\mathsf{K}^*/\mathsf{K})$, whence $\theta_{\varphi_1}(\mathfrak{A}) = \theta_\varphi(\mathfrak{A})$. Thus $(N_{\mathsf{K}/\mathsf{P}}\,\theta_\varphi)\,((a))$ solely depends on c and not on the actual choice of φ, and we can write

$$[d_1, d_2, a]_c = (N_{\mathsf{K}/\mathsf{P}}\,\theta_\varphi)\,((a)). \tag{3.3}$$

One can extend the definition of the new symbol by writing

$$[b_1^2 d_1, b_2^2 d_2, a]_c = [d_1, d_2, a]_c \tag{3.4}$$

whenever b_1, b_2 are non zero rationals. We may however always restrict our attention to the case $b_1 = b_2 = 1$.

Directly from the definitions we have

Theorem 5 (First Decomposition Theorem). *The domain of values of* $[d_1, d_2, a]_c$ *is* ± 1. — *If* $\{d_1, d_2, c\}$ *is non degenerate, and if* $a \in S(d_1, d_2, c)$ *then*

$$[d_1, d_2, a]_c = 1$$

if and only if for some (for every) $\varphi \in \Phi^*(d_1, d_2, c)$ *and for some (for every) primitive ideal* $\mathfrak{A}$ *in* K *with norm* (a)

$$(\mathsf{K}_\varphi/\mathsf{K}; \mathfrak{A}) = 1.$$

In particular if a *is a prime power then* (a) *is ideal norm of* K_φ *if and only if*

$$[d_1, d_2, a]_c = 1.$$

In view of this Theorem we shall refer to the symbol $[d_1, d_2, a]_c$ in all cases as the *decomposition symbol*. Together with ordinary quadratic residue symbols it will in the non degenerate case suffice to provide a decomposition criterion in $S(d_1, d_2, c)$ for every normal field of degree 8 containing $\mathsf{K} = \mathsf{P}(\sqrt{d_1}, \sqrt{d_2})$. We recall that every such field is of form K_φ with $\varphi \in \Phi_\mathsf{K}$.

Theorem 6 (Second Decomposition Theorem). *Let* d_1, d_2 *be independent quadratic discriminants,* $\mathsf{K} = \mathsf{P}(\sqrt{d_1}, \sqrt{d_2})$. *To every normal field* K_φ $(\varphi \in \Phi_\mathsf{K})$ *there belongs a triplet* $\{d_1, d_2, c\}$ *and a rational quadratic residue character* χ *with conductor* $\mathfrak{f}(\chi)$ *prime to* $d_1 d_2$, *and to every triplet* $\{d_1, d_2, c\}$ *and every such residue character* χ *there belongs a field* K_φ $(\varphi \in \Phi_\mathsf{K})$ *in the following sense:*

For every prime power $p^r \in S(d_1, d_2, c)$ *prime to* $\mathfrak{f}(\chi)$, (p^r) *is ideal norm of* K_φ *if and only if*

$$\chi(p^r)\,[d_1, d_2, p^r]_c = 1.$$

Proof. Let M be the group of rational idèle class characters μ with $\mu^2 = 1$ of conductor prime to $d_1 d_2$. Every character

$$\varphi = \varphi' R_{K/P}\mu \qquad (\varphi' \in \Phi_K^*,\ \mu \in M) \tag{3.5}$$

lies in Φ_K, and every character $\varphi \in \Phi_K$ has a representation (3.5) (cf. [4], Theorem 5). The theorem now follows by observing that when p^r satisfies the hypothesis of Theorem 6 then by (1.10)

$$(N_{K/P}\theta_\varphi)((p^r)) = (N_{K/P}\theta_{\varphi'})((p^r))\,(N_{K/P}\theta_{\varphi''})((p^r)),$$

with $\varphi'' = R_{K/P}\mu$. The first factor on the right is $[d_1, d_2, p^r]_c$ for $c = c_{\varphi'} = c_\varphi$ by Theorem 5. For the second factor we have from the definition of the mappings $N_{K/P}$, $R_{K/P}$ the equation $N_{K/}\,\theta_{\varphi''} = \theta_\mu$, and then by (1.6), $\theta_\mu((p^r)) = \chi_\mu(p^r)$. Finally we note that every rational quadratic residue character χ of conductor prime to $d_1 d_2$ is of form χ_μ for some $\mu \in M$.

Theorem 7 (First Uniqueness Theorem). *The ordered pair d_1, d_2 together with the character φ determine the class c and the character χ in Theorem 6 uniquely. Two characters $\varphi_1, \varphi_2 \in \Phi_K$ will determine the same class c and the same character χ if and only if $\varphi_1\varphi_2^{-1} \in \Phi(K^*/K)$.*

Proof. The first part follows by the uniqueness of φ' and μ in (3.5) for given $\varphi \in \Phi_K$ (cf. [4] Theorem 5).

For the second part we first note that the prime power ideals $\mathfrak{P}^r$ for which $|N_{K/P}\mathfrak{P}^r|$ lies in $S(d_1, d_2, c)$ are precisely those which split completely in K^*, disregarding powers of factors of $\mathfrak{d}_c$. Two characters φ_1, φ_2 will then determine the same class c and the same character χ if and only if for all such prime powers $\mathfrak{P}^r$, $\theta_{\varphi_1}(\mathfrak{P}^r) = \theta_{\varphi_1}(\mathfrak{P}^r)$ i.e. $\theta_{\varphi_1\varphi_2^{-1}}(\mathfrak{P}^r) = 1$ i.e. $\varphi_1\varphi_2^{-1} \in \Phi(K^*/K)$.

From our discussion we also obtain another characterisation of the symbol $[d_1, d_2, a]_c$.

Let $\{d_1, d_2, c\}$ be a non degenerate triplet and let χ be a quadratic residue character of conductor prime to $d_1 d_2$. There exists a unique field $\bar{A}$ of degree 2 (or 1) over K^*, which is absolutely normal such that

(i) *the prime powers p^r, prime to $\mathfrak{f}(\chi)$, which lie in $S(d_1, d_2, c)$ are precisely those rational prime powers for which (p^r) is ideal norm of K^* and which are prime to the relative discriminant of $\bar{A}/K^*$;*

(ii) *the prime powers p^r for which in addition $\chi(p^r)[d_1, d_2, p^r]_c = 1$ are precisely those for which (p^r) is an ideal norm of $\bar{A}$.*

§ 4.

We recall the definition of the isomorphisms g_π: $\Gamma(K/P)$, and of automorphism π^* in § 2. From equation (2.11) and from the definitions in § 3 we have

Theorem 8 (First Inversion Law). *Let $\pi \in \Sigma$ and let $\{d_1, d_2, c\}$ be non degenerate. Then $\{d_{\pi(1)}, d_{\pi(2)}, \pi^*(c)\}$ is non degenerate and $[d_1, d_2, a]_c = [d_{\pi(1)}, d_{\pi(2)}, a]_{\pi^*(c)}$ where the right hand side is defined whenever the left hand side is.*

Let $\varkappa$ be the permutation (1, 2). Then

$$\varkappa^* c(\gamma_1) = c(\gamma_2), \quad \varkappa^* c(\gamma_2) = c(\gamma_1), \quad \varkappa^* c(\gamma_1, \gamma_2) = c(\gamma_1, \gamma_2). \tag{4.1}$$

From Theorem 8 we have thus in particular

$$[d_1, d_2, a]_c = [d_2, d_1, a]_{\varkappa^*(c)}. \tag{4.2}$$

When $c(\gamma_1) = c(\gamma_2) = 0$, $c(\gamma_1, \gamma_2) = 1$ our symbol can be shown to coincide essentially with that defined by L. RÉDEI in [9]. In this case $c = \varkappa^*(c)$, and so

$$[d_1, d_2, a]_c = [d_2, d_1, a]_c. \tag{4.3}$$

This is one of the inversion formulae found by L. RÉDEI in [9].

On the basis of the first inversion law the uniqueness theorem 7 can now in the non Abelian case be strengthened to

Theorem 9 (Second Uniqueness Theorem). *Let $\{d_1, d_2, c\}$ be a non degenerate triplet with $c(\gamma_1, \gamma_2) = 1$. If χ is a rational quadratic residue character and $\{d_1', d_2', c'\}$ a triplet such that for all primes $p \in S(d_1, d_2, c) \cap \cap S(d_1', d_2', c')$ with $(p, \mathfrak{f}(\chi)) = 1$*

$$\chi(p)\,[d_1', d_2', p]_{c'} = [d_1, d_2, p]_c,$$

then for all such primes p, $\chi(p) = 1$, $\mathfrak{f}(\chi)$ is a divisor of $d_1 d_2$, and $\exists \pi \in \Sigma$ such that $d_i' = d_{\pi(i)}$ $(i = 1, 2)$, $c' = \pi^*(c)$.

Proof. We shall troughout restrict ourselves to primes which are not divisors of $d_1 d_2 d_1' d_2' \mathfrak{f}(\chi)$. We can write $\chi = \chi' \chi''$ where χ', χ'' are quadratic residue characters, $(\mathfrak{f}(\chi'), d_1 d_2) = 1$, $\mathfrak{f}(\chi'') \mid d_1 d_2$. For the primes in $S(d_1, d_2, c)$, $\chi'(p) = \chi(p)$. We may thus assume already that $(\mathfrak{f}(\chi), d_1 d_2) = 1$.

The primes in $R = S(d_1 d_2, c) \cap S(d_1' d_2', c')$ are precisely those which split (completely) in some Abelian field $\bar{K}$. Let $K = P(\sqrt{d_1}, \sqrt{d_2})$, $\varphi \in \Phi^*(d_1, d_2, c)$. Then those primes in R for which $[d_1, d_2, p]_c = 1$ are precisely those splitting in $K_\varphi \bar{K}$. Note that K_φ and so $K_\varphi \bar{K}$ is non Abelian, but normal.

On the other hand the primes in R for which $\chi(p)[d_1', d_2', p]_{c'} = 1$ are those splitting in some normal field $\bar{A}$. When $\{d_1', d_2', c'\}$ is degenerate this

follows directly from the definition, otherwise by Theorem 6. In the degenerate case $\bar{A}$ will be Abelian.

Assume now the hypothesis of the Theorem to hold. Then $\bar{A} = \bar{\mathsf{K}}\mathsf{K}_\varphi$. Hence $\bar{A}$ is non Abelian, and so $\{d_1', d_2', c'\}$ is non degenerate. Let $\mathsf{K}' = \mathsf{P}(\sqrt{d_1'}, \sqrt{d_2'})$ and choose a character $\varphi' \in \Phi_{\mathsf{K}'}$ so that $\mathsf{K}'_{\varphi'}$ belongs to $\{d_1', d_2', c'\}$ and χ in the sense[9]) of Theorem 6. Then $A = \bar{\mathsf{K}}\mathsf{K}'_{\varphi'} = \bar{\mathsf{K}}\mathsf{K}_\varphi$. Hence in the first place $\mathsf{K}'_{\varphi'}$ is non Abelian and so $c'(\gamma_1, \gamma_2) = 1$. Moreover on inspecting the Galois group $\Gamma(\bar{A}/\mathsf{P})$ we find that K as the maximal Abelian subfield of K_φ belongs to the centre of $\Gamma(\bar{A}/\mathsf{P})$; the same is true for K', i. e. $\mathsf{K} = \mathsf{K}'$. On applying a suitable permutation $\pi \in \Sigma$ we may assume that $d_1' = d_1$, $d_2' = d_2$. By the first uniqueness theorem it follows then that $c' = c$ and $\chi = 1$.

Theorem 10 (First Multiplication Law).

With $\{d_1, d_2, c_1\}$, $\{d_1, d_2, c_2\}$ *also* $\{d_1, d_2, c_1 c_2\}$ *is a triplet, and*

$$[d_1, d_2, a]_{c_1}[d_1, d_2, a]_{c_2} = [d_1, d_2, a]_{c_1 c_2},$$

where all symbols are defined, provided that two of them are defined.

Proof. By the definitions and by Theorem 1.

Theorem 11 (Second Multiplication Law).

$$[d_1, d_2, a]_c [d_1, d_2, b]_c = [d_1, d_2, ab]_c,$$

where all symbols are defined, provided that two of them are defined.

Proof. By the definitions and by (1. 9).

§ 5.

In this section we shall state a number of Theorems, whose proofs are to be given in a second paper.

We consider the quadratic subfield

$$\Omega = \mathsf{P}(\sqrt{d_1}) \tag{5. 1}$$

of the biquadratic field $\mathsf{K} = \mathsf{P}(\sqrt{d_1}, \sqrt{d_2})$. The generating automorphism of Ω will be denoted by τ. We have

$$\mathsf{K} = \Omega_\mu \tag{5. 2}$$

for a certain idèle class character μ in Ω. The set of characters ψ in Ω

[9]) Note that we may now also assume $(\mathfrak{f}(\chi), d_1' d_2') = 1$.

for which

$$R_{K/\Omega}\psi \in \Phi^*(d_1, d_2, c)$$

will be denoted by $\Psi^*(d_2, c)$.

We shall consider the residue characters in Ω associated with idèle class characters (cf. (1.4)). We write

$$\chi_\mu = \eta. \tag{5.3}$$

For any residue character χ we denote by $\chi_\mathfrak{p}$ the product of its $\mathfrak{p}$-components, $\mathfrak{p}$ running through the prime divisors of p in Ω. Then we have

Theorem 12 (Criterion for Residue Characters). *Let $c \in A(d_1, d_2)$. A residue character χ in Ω will be of form χ_ψ, $\psi \in \Psi^*(d_2, c)$, if and only if*

(i) *for all p: $\chi_p^2 = \eta_p^{c(\gamma_2)}$, $\chi_p^{t-1} = \eta_p^{c(\gamma_1, \gamma_2)}$;*

(ii) *for $(p, f_1) = 1$: $\chi_p \neq 1$ if and only if $p | f_2^{c(\gamma_1)} f_3^{c(\gamma_3)}$.*

In the case $c(\gamma_1) = c(\gamma_2) = 0$, $c(\gamma_1, \gamma_2) = 1$ it follows that the characters $\chi_\psi (\psi \in \Psi^*(d_2, c))$ are precisely the quadratic residue symbols whose denominator is a primitive ideal with norm (d_2). From this it follows that for the given value of c our symbol coincides essentially with that of L. RÉDEI (cf. [9]). Moreover one gets in analogy to L. RÉDEI's result:

Theorem 13 (Second Inversion Law). *Let $\{d_1, d_2, c\}$, $\{d_1, d, c\}$ be triplets with $c(\gamma_1, \gamma_2) = 1$, $c(\gamma_1) = c(\gamma_2) = 0$. If both decomposition symbols are defined then*

$$[d_1, d_2, d]_c = [d_1, d, d_2]_c t$$

where $t = 1$ unless d_1, d_2, d are all distinct from 1, and either $d_2 < 0$ or $d < 0$. In this latter case we may assume without loss of generality that $d < 0$ and that $\left(\frac{-1, d_i}{p}\right) = 1$ for all p and for $i = 1, 2$. Then

$$t = \left[\frac{-1}{d_1}\right] \text{ if } d_2 = d_1; \quad t = \left[\frac{f_1}{d_1}\right]\left[\frac{f_2}{d_2}\right]\left[\frac{f_3}{d_3}\right]\left[\frac{-1}{f_3}\right]\left(\frac{f_2}{f_3}\right) \text{ if } d_1 \neq d_2.$$

Theorem 14 (Third Multiplication Law). *Let $c(\gamma_1) = 0$. If $\{d_1, d_2, c\}$, $\{d_1, d_2', c\}$, are triples, and if $d_2'' = d_2 d_2'/(d_2, d_2')^2$ then also $\{d_1, d_2'', c\}$ is a triplet, and*

$$[d_1, d_2, a]_c [d_1, d_2', a]_c = [d_1, d_2'', a]_c,$$

where all symbols are defined provided that two of them are defined.

By combining the stated multiplication and inversion laws one can derive further such laws, and in particular a multiplication law for the first argument d_1.

In conclusion we give explicit expressions for the decomposition symbol. For completeness sake we first deal with the case when the fields belonging to the given triplet are Abelian. Throughout all that follows $\{d_1, d_2, c\}$ is a given, non-degenerate triplet.

Theorem 15 (Explicit Form in the Abelian Case). *Let* $c(\gamma_1, \gamma_2) = 0$. *Then*

$$[d_1, d_2, a]_c = \begin{cases} \left[\frac{a}{d_1}\right]\left[\frac{-1}{d_1}\right]^{(\operatorname{sign} a-1)/2} & \text{if} \quad c(\gamma_1)=1,\ c(\gamma_2)=0, \\ \left[\frac{a}{d_2}\right]\left[\frac{-1}{d_2}\right]^{(\operatorname{sign} a-1)/2} & \text{if} \quad c(\gamma_1)=0,\ c(\gamma_2)=1, \\ \left[\frac{a}{d_3}\right]\left[\frac{-1}{d_3}\right]^{(\operatorname{sign} a-1)/2} & \text{if} \quad c(\gamma_1)=c(\gamma_2)=1, \\ 1 & \text{if} \quad c(\gamma_1)=c(\gamma_2)=0. \end{cases}$$

For the non Abelian case we first observe that every element in $S(d_1, d_2, c)$ is the product of elements a^r and p^{2s} of the following types:

(i) a is a square free integer in $S(d_1, d_2, c)$.

(ii) p is a prime, $p \notin S(d_1, d_2, c)$ but $p^2 \in S(d_1, d_2, c)$. By Theorem 11 it will thus suffice to give explicit forms for elements of these two types only.

Theorem 16 (Explicit Form for Prime Squares). *Let* $c(\gamma_1, \gamma_2) = 1$ *and let* p^2 *be of type* (ii).

(a) *If* $(p, d_1 d_2) = 1$ *then*

$$[d_1, d_2, p^2]_c = \begin{cases} \left(\frac{p}{d_i}\right)^{e(\gamma_2)} (i=2,3) & \text{when} \quad \left(\frac{p}{d_1}\right)=1, \\ \left(\frac{p}{d_i}\right)^{e(\gamma_1)} (i=1,3) & \text{when} \quad \left(\frac{p}{d_2}\right)=1, \\ \left(\frac{p}{d_i}\right)^{e(\gamma_3)} (i=1,2) & \text{when} \quad \left(\frac{p}{d_3}\right)=1. \end{cases}$$

(b) *If* $p \mid d_1 d_2$ *then* $[d_1, d_2; p^2]_c = 1$.

For square free integers we shall use a representation by ternary quadratic forms, which is easily derived from the theory of quadratic fields.

Proposition 5.1. *For every square free integer* a *with* $\left(\frac{a, d_1}{p}\right) = 1$ *for all* p, *there exist rational integers* $2x, 2y, z$ *such that*

(i) $x^2 - y^2 d_1 - z^2 a = 0$,

(ii) $x - y$ *is an integer and* $(2x, 2y, x-y) = 1$,

(iii) $z > 0$, $(z, a d_1 d_2) = 1$ *and* $\left(\frac{z, d_1}{p}\right) = 1$ *for all* $p \mid z$.

Assume now that $a \in S(d_1, d_2, c)$, $c(\gamma_1, \gamma_2) = 1$. Then we get:

Proposition 5.2. *Let* $p|f_1$. *If* $p^{c(\gamma_2)} \equiv 3 \pmod 4$ *then*

$$\left(\frac{d_1}{p}\right) = -1, \quad (a, p) = 1, \quad \left(\frac{a}{p}\right) = 1. \tag{5.4}$$

If $p^{c(\gamma_2)} \equiv 1 \pmod 4$ *then* $\left(\frac{d_1}{p}\right) = 1$ *so that* $\exists e$ *with*

$$d_1 \equiv e^2 \pmod p. \tag{5.5}$$

Moreover if x, y, z *give a representation of* a *as in Proposition 5.1 then* e *can be chosen so that*

$$(x + ye, p) = 1. \tag{5.6}$$

If $(p, a) = 1$, (5.6) of course will hold for all possible values of (5.5); the existence of a suitable e when $p|a$ follows from a more detailed analysis of the conditions in Proposition 5.1. The remainder of Proposition 5.2 is immediate from the definitions.

Let now $2x, 2y, z$ give a representation of a as in Proposition 5.1 and let $p|f_1$. We define a symbol

$$\left\{ \frac{x, y}{p} \right\}_{d_1}.$$

In the second case possible by Proposition 5.2, namely when $\left(\frac{d_1}{p}\right) = 1$, we write

$$\left\{ \frac{x, y}{p} \right\}_{d_1} = \left(\frac{x + ye}{p}\right) \tag{5.7}$$

with e satisfying (5.5), (5.6). If $p|a$ then e is uniquely determined mod p. If $p \nmid a$ then $\left(\frac{a}{p}\right) = 1$ and so the value of the right hand side in (5.7) will remain unaltered if e is replaced by $-e$. Thus in all cases the left hand side is not affected by the possible choices of e.

The other possible case is (5.4). Then

$$\left(\frac{x^2 - y^2 d_1}{p}\right) = 1$$

and so there exist integers u, v such that

$$u^2 + v^2 d_1 \equiv x, \quad 2uv \equiv y \pmod p. \tag{5.8}$$

The value of the symbol

$$\left\{ \frac{x, y}{p} \right\}_{d_1} = \left(\frac{u^2 - v^2 d_1}{p}\right) \tag{5.9}$$

is then independent of the particular choice of u and v.

We shall write f_1' for the product of the primefactors of f_1 which are $\equiv 1 \pmod 4$. Then we have

Theorem 17 (Explicit Form for Square Free Integers). *Let* $c(\gamma_1, \gamma_2) = 1$ *and let* a *be a square free integer in* $S(d_1, d_2, c)$. *Then for every representation of* a *as in Proposition 5.1*

$$[d_1, d_2, a]_c = rs$$

is the product of a "residue factor" r *and a "signature factor"* s.

The residue factor is given by

$$r = \begin{cases} \left(\frac{x}{f_3}\right) \prod_{p|f_1} \left\{\frac{x,y}{p}\right\}_{d_1} & \text{when } c(\gamma_1) = c(\gamma_2) = 0, \\ \left(\frac{x}{f_2}\right) \prod_{p|f_1} \left\{\frac{x,y}{p}\right\}_{d_1} & \text{when } c(\gamma_1) = 1,\ c(\gamma_2) = 0, \\ \left(\frac{z}{d_2}\right)\left[\frac{az^2}{f_1'}\right] \prod_{p|f_1} \left\{\frac{x,y}{p}\right\}_{d_1} & \text{when } c(\gamma_1) = 0,\ c(\gamma_2) = 1, \\ \left(\frac{x}{d_1}\right)\left(\frac{z}{d_2}\right)\left[\frac{az^2}{f_1'}\right] \prod_{p|f_1} \left\{\frac{x,y}{p}\right\}_{d_1} & \text{when } c(\gamma_1) = c(\gamma_2) = 1. \end{cases}$$

The signature factor is given by

$$s = \left\{\left[\frac{-1}{d_1}\right]^{c(\gamma_1)}\left[\frac{-1}{d_2}\right]^{c(\gamma_2)}\left[\frac{f_1}{d_1}\right]\left[\frac{f_2}{d_2}\right]\left[\frac{f_3}{d_3}\right]\left[\frac{-1}{f_3}\right]\left(\frac{f_2}{f_3}\right)\right\}^{(\operatorname{sign} \alpha - 1)/2}$$

when all prime divisors of $d_1 d_2$ *are* $\equiv 1 \pmod 4$, *by* $s = (-1)^{(\operatorname{sign} \alpha - 1)/2}$ *when* $d_1 > 0$, $d_2 < 0$, *and by* $s = 1$ *in all other cases.*

An important feature of this theorem is the *invariance of value* of the explicit expressions given for rs; though these involve functions of x, y, z they are in fact quite independent of the particular choice of these parameters. Moreover the inversion laws, and in particular the second inversion law and the special formula (4.2) arising out of the first inversion law lead now to *reciprocity formulae* for the explicit expressions given in the theorem. Both these phenomena were already noted in a similar context in [3]. Finally the multiplication laws for the decomposition symbol, and in particular Theorem 11 exhibit a multiplicative property of the expressions given in the last theorem. Conversely of course some of the earlier theorems (e. g. Theorem 10) can in turn be derived from Theorem 15—17.

References

[1] C. Chevalley, Théorie du corps de classes, *Annals of Math.*, (2) **41** (1940), 394—418.
[2] A. Fröhlich, On fields of class two, *Proc. London Math. Soc.*, (3) **4** (1954), 235—256.
[3] A. Fröhlich, The restricted biquadratic residue symbol, *Proc. London Math. Soc.*, (3) **9** (1959), 189—207.
[4] A. Fröhlich, The rational characterization of certain sets of relatively Abelian extensions, *Philosophical Transactions Royal Soc. London*, (A) **251** (1959), 385—425.
[5] Y. Furuta, A reciprocity law of the power residue symbol, *Journ. Math. Soc. Japan*, **10** (1958), 46—54.
[6] Y. Furuta, On meta-abelian fields of a certain type, *Nagoya Math. Journal*, **14** (1959), 193—199.
[7] S. Kuroda, Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoisschen Körpern, *Journal Math. Soc. Japan*, **3** (1951), 148—156.
[8] L. Rédei, Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *Journal f. d. reine u. angew. Math.*, **171** (1934), 131—148.
[9] L. Rédei, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper, *Journal f. d. reine u. angew. Math.*, **180** (1939), 1—43.
[10] L. Rédei, Bedingtes Artinsches Symbol mit Anwendung in der Klassenkörpertheorie, *Acta Math. Acad. Sci. Hung.*, **4** (1953), 1—29.
[11] L. Rédei, Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung, *Acta Math. Acad. Sci. Hung.*, **4** (1953), 31—87.

KING'S COLLEGE,
LONDON

(Received February 11, 1960)

Über die Nichteinfachheit von faktorisierbaren Gruppen

Von J. SZÉP in Szeged

Prof. L. Rédei zum 60. Geburtstag gewidmet

Da es unendlich viele faktorisierbare einfache Gruppen gibt, spielt in der Theorie der faktorisierbaren Gruppen — wie auch in der Gruppentheorie überhaupt — die Frage der Nichteinfachheit eine wichtige Rolle. Bezüglich mehreren Klassen von faktorisierbaren Gruppen ist es bekannt, daß sie nichteinfach [6], ja sogar auflösbar sind [1], [2], [3], [8], [9]. Die Aufgabe entbehrt also nicht des Interesses, nach solchen Kriterien zu suchen, welche die Nichteinfachheit faktorisierbarer Gruppen gewährleisten. Die Untersuchung dieser Frage ist außerdem auch noch darum von Interesse, weil in gewißen Fällen die Nichteinfachheit die Auflösbarkeit der betreffenden faktorisierbaren Gruppe nach sich zieht. Zur Unterstützung dieser Behauptung mag folgender Gedankengang (der in speziellen Fällen schon in früheren Arbeiten angewandt ist) dienen:

Es sei $G = AB$ eine endliche faktorisierte Gruppe, wobei die Ordnungen der Gruppen A und B zueinander relativ prim sind. Es sollen A und B, sowie auch sämtliche Normalteiler und Faktorgruppen dieser beiden Gruppen eine gewiße Eigenschaft $\mathfrak{A}$ besitzen. Man sieht ohne Schwierigkeit ein, daß aus der Nichteinfachheit aller Gruppen mit der Eigenschaft $\mathfrak{A}$ (für die Faktoren) die Auflösbarkeit von G folgt. Den Beweis führen wir durch vollständige Induktion. Nehmen wir an, daß die Auflösbarkeit für faktorisierbare Gruppen der Eigenschaft $\mathfrak{A}$ und einer niedrigeren Ordnung als G bereits bewiesen ist. Es sei N ein Normalteiler von G. Dann gilt $N = N_1 N_2$ wo N_1 Normalteiler von A, und N_2 Normalteiler von B ist [5], und es ist $G/N \approx \approx A/N_1 B/N_2$. Der Induktionsvoraussetzung gemäß sind G/N und N auflösbare Gruppen, und folglich ist auch G auflösbar.

Bei unserer Untersuchung spielt der schon auch von anderen Verfassern oft benutzte folgende Satz eine wichtige Rolle:

Satz A ([4] oder [7]). *$G = AB$ ist nicht einfach, wenn $A \cap B$ einen Normalteiler $\neq 1$ von A oder B enthält.*

Wir werden noch zwei Hilfssätze benutzen, die wir der Vollständigkeit halber beweisen werden, obwohl sie schon in einer früheren Arbeit [6] vorgekommen sind. Den Hilfssätzen schicken wir folgendes voran.

Die Elemente einer vorgelegten Gruppe $G = AB (= BA)$ können wir als $a_i b_k$ und $b_l a_s$ $(a_i, a_s \in A;\ b_k, b_l \in B)$ darstellen. Ist $A \cap B = 1$, so durchläuft das Element a_i' in $a_i b = b_i a_i'$ $(i = 1, 2, \ldots)$ zusammen mit a_i bei festem b $(b, b_i \in B)$ alle Elemente von A. Wir bezeichnen durchweg mit $[b]$ das durch b eindeutig bestimmte System der b_i in $a_i b = b_i a_i'$ $(i = 1, 2, \ldots)$; dabei zählen wir die Elemente b_i mit Multiplizität.

Hilfssatz 1. *Ist* $\bar{b} \in [b]$, *so ist* $[\bar{b}] = [b]$.

Beweis. Wegen $b \in [b]$ gilt eine Gleichung $ab = \bar{b}a'$ $(a, a' \in A;\ b, \bar{b} \in B)$. Setzen wir das Element $b = a^{-1}\bar{b}a'$ in die Gleichungen $a_i b = b_i a_i'$ $(i = 1, 2, \ldots)$ ein, so bekommen wir die Gleichungen $a_i a^{-1}\bar{b} = b_i a_i' a'^{-1}$ aus welchen die Behauptung folgt.

Hilfssatz 2. $[b]$ *enthält alle seine Elemente mit gleicher Multiplizität.*

Beweis. Wir fassen unter allen Gleichungen $a_i b = b_i a_i'$ $(i = 1, 2, \ldots)$ diejenigen ins Auge, für welche $b_i = b$ ist. Gilt $b_i = b$ für alle i so ist die Behauptung des Hilfssatzes trivial. Es sei dann $a_k b = b_k a_k$ eine Gleichung, wo $b_k \neq b$ gilt. Setzen wir das Element $b = a_k^{-1} b_k a_k'$ in die rechte Seite jeder Gleichung $\bar{a}_i b = b\bar{a}_i'$ $(i = 1, 2, \ldots)$ ein, so bekommen wir die Gleichungen $a_k a_i b = b_k a_k' \bar{a}_i'$ $(i = 1, 2, \ldots)$. Es folgt aus diesen Gleichungen, daß die Multiplizität von b_k in $[b]$ nicht kleiner, als die von b. Andererseits wählen wir für festes k die Gleichungen $\bar{a}_i b = b_k \bar{a}_i'$ $(i = 1, 2, \ldots)$ aus den Gleichungen $a_i b = b_i a_i'$ aus. Setzen wir das Element $b_k = a_k b a_k'^{-1}$ in die Gleichungen $\bar{a}_i b = b_k \bar{a}_i'$ $(i = 1, 2, \ldots)$ ein, so entstehen die Gleichungen $a_k^{-1}\bar{a}_i b = b a_k'^{-1}\bar{a}_i'$ $(i = 1, 2, \ldots)$ also ist die Multiplizität von b in $[b]$ nicht kleiner, als die von b_k. Somit haben wir Hilfssatz 2 bewiesen.

Satz 1. *Es sei* $G = AB$ $(A \cap B = 1)$ *eine faktorisierte Gruppe. Es seien* N_A *und* N_A' *je ein Normalteiler von* A *und* $Z_B (\neq 1)$ *das Zentrum von* B. *Gilt* $b^{-1} N_A b = N_A'$ *für ein* $b \neq 1$ *aus* Z_B, *so ist* G *nicht einfach.*

Beweis. Wir unterscheiden zwei Fälle, je nach dem die von $[b]$ erzeugte Gruppe $\{[b]\}$ eine echte Untergruppe von B ist oder nicht.

Fall 1. $[b]$ erzeugt nicht die Gruppe B. In diesem Fall ergibt sich (mit Verwendung des Hilfssatzes 1 und der Gleichungen $a_i b = b_i a_i'$) $A\{[b]\} = \{[b]\}A = A' \subset G$, also ist $G = A'B$. Da der Normalteiler $\{b\}$ von B in $A' \cap B$ liegt, ist nach Satz A die Gruppe G nicht einfach.

Fall 2. $[b]$ erzeugt die Gruppe B. Wir werden mehrere Unterfälle unterscheiden:

a) Ist $b_i = b$ $(i = 1, 2, \ldots; b_i \in [b])$, so ist $b^{-1}Ab = A$, also ist A Normalteiler von G.

b) Gibt es ein l mit $[b] \ni b_l \neq b$, so ist $N_A b_l b^{-1} = b_l b^{-1} N_A$. Setzen wir nämlich das Element $b = a_l^{-1} b_l a_l'$ in $N_A b = b N_A'$ ein, so ergibt sich $N_A b_l = b_l N_A'$. Aus dieser Gleichung und aus $N_A b = b N_A'$ folgt die Behauptung. Man sieht auch, daß N_A durch $b_l b^{-1}$ also auch durch alle Elemente von $[b_i b^{-1}]$ $(i = 1, 2, \ldots; b_i \in [b])$ in sich transformiert wird.

Man bezeichne mit B' die durch die Elemente sämtlicher Komplexe $[b_i b^{-1}]$ $(i = 1, 2, \ldots)$ erzeugte Gruppe.

b_1) Ist $B' = B$, so ist die Gruppe N_A Normalteiler in G.

b_2) Ist $B' \subset B$, so gilt $B' \not\ni b$ (wegen $\{[b_1 b^{-1}], [b_2 b^{-1}], \ldots, b\} \supseteq \{b_1 b^{-1}, b_2 b^{-1}, \ldots, b\} \supseteq \{[b]\} = B$). Es ist ferner klar, daß $\{[b_1 b^{-1}], [b_2 b^{-1}], \ldots\}\{b\} \supseteq \{b_1 b^{-1}, b_2 b^{-1}, \ldots\}\{b\} \supseteq \{[b]\} = B$ gilt, also ist $\{[b_1 b^{-1}], [b_2 b^{-1}], \ldots\}\{b\} = B$ und $AB' = B'A \neq G$. Folglich gilt $G = AB = (AB')(B'\{b\})$, $AB' \cap B'\{b\} = B'$. Die Gruppe B' ist Normalteiler in $B'\{b\}$ $(= B)$, also ist G nach Satz A nicht einfach. Damit ist Satz 1 bewiesen.

Satz 2. *Es sei $G = AB$ $(A \cap B = 1)$ eine endliche faktorisierte Gruppe. Es sei N_A ein Normalteiler von A mit der Eigenschaft, daß jede Untergruppe von N_A ein Normalteiler von A ist. Es sei weiterhin $Z_B (\neq 1)$ das Zentrum von B. Gilt $N_A Z_B' = Z_B' N_A$ $(Z_B' \neq 1; Z_B' \subseteq Z_B)$ mit $|Z_B'| \not\equiv 1 \pmod{|N_A|}$ so ist G nicht einfach; dabei bedeutet $|\ldots|$ die Anzahl der Verschieden Elemente der eingeklammerten Menge.*

Beweis. Es ist klar, daß N_A eine Hamiltonsche Gruppe ist. Betrachten wir die Gleichungen $a_i b = b_i a_i'$ $(a_i, a_i' \in N_A; b, b_i \in Z_B')$. Aus ihnen folgt, daß jeder Komplex $[b_i]$ höchstens $|N_A|$ verschiedene Elemente enthält; dieser Grenzfall tritt genau dann ein, wenn die Multiplizität der Elemente in $[b_i]$ den Wert 1 hat. Nach Hilfssatz 1 und 2 kann nicht jeder Komplex $[b_i]$ $(b_i \in Z_B')$ genau $|N_A|$ verschiedene Elemente haben. Denn sonst hätte Z_B' nach Hilfssatz 1 eine Zerlegung

$$Z_B' = [1] + [b'] + [b''] + \cdots \qquad (b', b'', \ldots \in Z_B')$$

mit $|[1]| = 1$, $|[b']| = |[b'']| = \cdots = |N_A|$. Dies widerspricht aber der Bedingung $|Z_B'| \not\equiv 1 \pmod{|N_A|}$.

Z_B' hat also ein Element b, dessen Multiplizität in $[b]$ mindestens zwei ist, also gilt eine Gleichung $N_A' b = b N_A'$ $(N_A', N_A' \subseteq N_A)$. Nach Satz 1 ist also die Gruppe G nicht einfach.

Bemerkung. Die Bedingung $|Z_B'| \not\equiv 1 \pmod{|N_A|}$ ist z. B. dann trivialerweise befriedigt, wenn $|Z_B'| \leqq |N_A'|$ oder $(|Z_B'|, |N_A|) \neq 1$ ist.

Korollar 1. *Es sei* $G = AB$ $(A \cap B = 1)$ *eine endliche Gruppe. Es sei* Z_A $(\neq 1)$ *bzw.* Z_B $(\neq 1)$ *das Zentrum von* A *bzw.* B. *Wenn es Untergruppen* $Z'_A \neq 1$ *und* $Z'_B \neq 1$ *in* Z_A *bzw.* Z_B *gibt für welche* $Z'_A Z'_B = Z'_B Z'_A$ *ist, so ist* G *nicht einfach.*

Beweis. Wir können $|Z'_A| \geqq |Z'_B|$ annehmen. Nach der vorigen Bemerkung ist die Bedingung $|Z'_B| \not\equiv 1 \pmod{|Z'_A|}$ befriedigt, also ist G nach Satz 2 nicht einfach.

Korollar 2.*) *Eine endliche Gruppe* $G = AB$ *ist nicht einfach, wenn* A *eine Abelsche Gruppe ist,* B *ein Zentrum* $(\neq 1)$ *hat und* $|A| \geqq |B|$ *gilt.*

Beweis. Ist $A \cap B \neq 1$, so ist $A \cap B$ ein Normalteiler von A, also ist G nach Satz A nicht einfach. Im Fall $A \cap B = 1$ sei b $(\neq 1)$ ein Element des Zentrums von B. In den Gleichungen $a_i b = b_i a'_i$ $(a_i, a'_i \in A;\ b, b_i \in B)$ sind wegen $|A| \geqq |B|$ nicht alle b_i verschieden, folglich ist nach Hilfssatz 2 die Multiplizität von b in $[b]$ mindestens zwei. Die Gruppe A hat also zwei Untergruppen A', A'' $(\neq 1)$, für welche $b^{-1} A' b = A''$ gilt. Also ist G nach Satz 1 nicht einfach.

Literaturverzeichnis

[1] B. Huppert, Über die Auflösbarkeit faktorisierbarer Gruppen, *Math. Zeitschrift*, **59** (1953), 1—7.

[2] C. Huppert—N. Itô, Über die Auflösbarkeit faktorisierbarer Gruppen. II, *Math. Zeitschrift*, **61** (1954), 94—99.

[3] N. Itô, Remarks on factorisable groups, *Acta Sci. Math.*, **14** (1951), 83—84.

[4] O. Ore, Contributions to the theory of finite order, *Duke Math. Journal*, **5** (1939), 431—460.

[5] J. Szép, On the structure of groups which can be represented as the product of two subgroups, *Acta Sci. Math.*, **12 A** (1950), 57—61.

[6] J. Szép, Zur Theorie der faktorisierbaren Gruppen, *Acta Sci. Math.*, **16** (1955), 54—57.

[7] J. Szép—L. Rédei, On factorisable groups, *Acta Sci. Math.*, **13** (1950), 235—238.

[8] H. Wielandt, Über das Produkt paarweise vertauschbarer nilpotenter Gruppen, *Math. Zeitschrift*, **55** (1951), 1—7.

[9] H. Wielandt, Über Produkte von nilpotenter Gruppen, *Illinois Journal of Math.*, **2** (1958), 611—618.

(Eingegangen am 29. Februar 1960)

*) Dieser Satz wurde schon in der Arbeit [6] auf ähnliche Weise bewiesen.

Sur les contractions de l'espace de Hilbert. IV

Par BÉLA SZ.-NAGY à Szeged et CIPRIAN FOIAŞ à Bucarest

Dédié au 60ième anniversaire de M. le professeur L. Rédei

Le but de cet article est de montrer que toute contraction T de l'espace de Hilbert est la somme orthogonale[1]) d'une transformation unitaire $T^{(u)}$ et d'une contraction "complètement non-unitaire" $T^{(0)}$ et d'étudier la dilatation unitaire $U^{(0)}$ de $T^{(0)}$. On verra que $U^{(0)}$ est unitairement équivalente à une somme orthogonale $\bigoplus_{\omega} V(M_\omega)$ où $V(M_\omega)$ désigne la multiplication par $e^{i\theta}$ dans l'espace $L^2(M_\omega)$ des fonctions $f(\theta)$ définies dans l'ensemble mesurable $M_\omega \subseteq [0, 2\pi]$. Des résultats analogues seront obtenus pour les semi-groupes à un paramètre de contractions.

1. Cas d'une seule contraction

Rappelons[2]) que pour toute contraction T de l'espace de Hilbert $\mathfrak{H}$ il existe une transformation unitaire U d'un espace de Hilbert $\mathfrak{K}$ contenant $\mathfrak{H}$ comme un sous-espace, telle qu'on ait

$$T^n = \mathrm{pr}_{\mathfrak{H}} U^n \qquad (n = 0, 1, 2, \ldots)$$

et que $\mathfrak{K}$ soit sous-tendu par les éléments de la forme $U^n h$ $(h \in \mathfrak{H}; n = 0, \pm 1, \pm 2, \ldots)$. La structure $\{\mathfrak{K}, U, \mathfrak{H}\}$ est déterminée à isomorphie près; U s'appelle la *dilatation unitaire* de la contraction T.

Faisons la remarque évidente que la dilatation unitaire d'une somme orthogonale $\bigoplus_{\omega} T^{(\omega)}$ de contractions est égale à la somme orthogonale $\bigoplus_{\omega} U^{(\omega)}$ des dilatations unitaires correspondantes.

Une transformation linéaire bornée T de l'espace $\mathfrak{H}$ sera appelée *complètement non-unitaire* si pour tout élément $h \neq 0$ de l'espace $\mathfrak{H}$ les quantités

$$\|Th\|, \|T^2 h\|, \ldots, \|T^n h\|, \ldots; \quad \|T^* h\|, \|T^{*2} h\|, \ldots, \|T^{*n} h\|, \ldots$$

ne sont pas toutes égales à $\|h\|$.

[1]) Ou "somme directe".

[2]) Cf. les articles précédents [2—5].

Théorème 1.[3]) *A toute contraction T de l'espace $\mathfrak{H}$ correspond une décomposition de $\mathfrak{H}$ en somme orthogonale de deux sous-espaces orthogonaux complémentaires $\mathfrak{H}^{(u)}$ et $\mathfrak{H}^{(0)}$ réduisant T et tels que la partie de T dans $\mathfrak{H}^{(u)}$ est une transformation unitaire $T^{(u)}$ et sa partie dans $\mathfrak{H}^{(0)}$ est une contraction complètement non-unitaire $T^{(0)}$. Cette décomposition est unique, $\mathfrak{H}^{(u)}$ étant constitué des éléments h pour lesquels*

$$\|T^n h\| = \|h\| = \|T^{*n} h\| \quad \textit{pour} \quad n = 1, 2, \ldots . \tag{1}$$

[4])

$T^{(u)}$ et $T^{(0)}$ seront appelées la *partie unitaire* et la *partie complètement non-unitaire* de T.

Démonstration. Soit U la dilatation unitaire de T. Envisageons l'ensemble $\mathfrak{H}^{(u)}$ des éléments h de $\mathfrak{H}$ vérifiant (1). Comme on a $T^n h = PU^n h$ [5]) et $T^{*n} = PU^{-n}h$ $(n = 0, 1, 2, \ldots)$, et comme $\|U^n h\| = \|h\|$ $(n = 0, \pm 1, \pm 2, \ldots)$ puisque U est unitaire, la condition (1) est équivalente à ce que

$$U^n h \in \mathfrak{H} \quad \text{pour} \quad n = 0, \pm 1, \pm 2, \ldots .$$

Cela veut dire que

$$\mathfrak{H}^{(u)} = \bigcap_{-\infty < n < \infty} U^{-n}\mathfrak{H}. \tag{2}$$

La formule (2) met en évidence que $\mathfrak{H}^{(u)}$ est un sous-espace de $\mathfrak{H}$ qui est appliqué par U et par U^{-1} sur lui-même. Comme dans $\mathfrak{H}^{(0)}$ U coïncide avec T et U^{-1} avec T^*, il en résulte que $\mathfrak{H}^{(u)}$ réduit T, et que la partie $T^{(u)}$ de T dans $\mathfrak{H}^{(u)}$ est unitaire. La partie de T dans le sous-espace complémentaire $\mathfrak{H}^{(0)}$, soit $T^{(0)}$, est alors — par la définition même de $\mathfrak{H}^{(u)}$ — complètement non-unitaire. Si $\mathfrak{H} = \mathfrak{H}' \oplus \mathfrak{H}''$ est une décomposition quelconque de $\mathfrak{H}$ en somme orthogonale de deux sous-espaces réduisant T, tels que la partie de T dans $\mathfrak{H}'$ soit unitaire et la partie dans $\mathfrak{H}''$ complètement non-unitaire, la condition (1) est vérifiée pour tous les éléments de $\mathfrak{H}'$ (puisque T y est unitaire), donc $\mathfrak{H}' \subseteq \mathfrak{H}^{(u)}$, et s'il y avait dans $\mathfrak{H}^{(u)}$ un élément $h \neq 0$, orthogonal à $\mathfrak{H}'$, h devrait appartenir à la fois à $\mathfrak{H}^{(u)}$ et à $\mathfrak{H}''$, ce qui est impossible puisque dans $\mathfrak{H}''$, T est complètement non-unitaire. Donc $\mathfrak{H}' = \mathfrak{H}^{(u)}$, $\mathfrak{H}'' = \mathfrak{H}^{(0)}$, ce qui achève la démonstration.

La dilatation unitaire de T est alors égale à $T^{(u)} \oplus U^{(0)}$ où $U^{(0)}$ est la dilatation unitaire de $T^{(0)}$, définie dans un espace $\mathfrak{K}^{(0)} \supseteq \mathfrak{H}^{(0)}$. Cela impose le

---

[3]) Ce théorème a été établi indépendamment aussi par M. Heinz Langer (Dresden), *voir* sa Note à paraître dans les *Acta Math. Acad. Sci. Hung.*

[4]) $\mathfrak{H}^{(u)}$ ou $\mathfrak{H}^{(0)}$ peut se réduire au seul élément 0.

[5]) On désignera par P toujours la projection orthogonale sur $\mathfrak{H}$, sous-espace de l'espace de dilatation $\mathfrak{K}$.

problème d'étudier les dilatations unitaires des contractions complètement non-unitaires de plus près.

Théorème 2. *La dilatation unitaire U d'une contraction complètement non-unitaire T a son spectre absolument continu. D'une manière plus précise, U est unitairement équivalente à une somme orthogonale de type $\bigoplus_{\omega\in\Omega} V(M_\omega)$ où $V(M_\omega)$ désigne la multiplication par $e^{i\theta}$ dans l'espace $L^2(M_\omega)$ des fonctions $f(\theta)$ définies dans un ensemble mesurable $M_\omega \subseteq [0, 2\pi]$.*

Démonstration. Soient $\mathfrak{H}$ et $\mathfrak{K}$ les espaces de Hilbert où T et U sont définies et soit $U = \int_0^{2\pi} e^{i\theta} dE_\theta$ la décomposition spectrale de U, la famille spectrale $\{E_\theta\}$ étant choisie continue de droite et telle que $E_0 = E_{+0} = O$ (la transformation nulle de l'espace $\mathfrak{K}$). L'assertion que U a son spectre absolument continu veut dire que pour tout $f \in \mathfrak{K}$ la fonction numérique non-décroissante $(E_\theta f, f)$ est absolument continue dans l'intervalle $0 \leqq \theta \leqq 2\pi$.

Soit $\{E(\sigma)\}$ la mesure spectrale engendrée par la famille spectrale $\{E_\theta\}$, définie pour tout ensemble borélien $\sigma \subseteq [0, 2\pi]$, c'est-à-dire que

$$E(\sigma) = \int_0^{2\pi} \chi(\sigma; \theta) dE_\theta$$

où $\chi(\sigma; \theta)$ est la fonction caractéristique de l'ensemble σ.

En désignant la mesure de Lebesgue d'un ensemble borélien σ par $m(\sigma)$, montrons tout d'abord que pour un ensemble σ *fermé* et de mesure $m(\sigma) = 0$ on a $E(\sigma) = O$.

Nous faisons usage à cette fin du fait qu'il existe une fonction à valeurs complexes $u(\sigma; \lambda)$ vérifiant les conditions suivantes: elle est continue dans le disque fermé unité

$$S_0 = \{\lambda : |\lambda| \leqq 1\}$$

du plan des nombres complexes, holomorphe dans l'intérieur de S_0, égale à 1 aux points $\lambda = e^{i\theta}$ de la circonférence pour lesquels $\theta \in \sigma$, et de module plus petit que 1 en tous les autres points λ de S_0. L'existence de telle fonction a été démontrée par F. et M. Riesz ([1], p. 36—37); ils sont partis d'une construction due à Fatou.

On a pour tout $f \in \mathfrak{K}$, par le théorème de Lebesgue,

$$\|[u(\sigma; U)]^n f - E(\sigma) f\|^2 = \int_0^{\pi 2} |[u(\sigma; e^{i\theta})]^n - \chi(\sigma; \theta)|^2 d(E_\theta f, f) \to 0 \qquad (n \to \infty)$$

donc

$$[u(\sigma; U)]^n \to E(\sigma)$$

et par conséquent

$$\mathrm{pr}_{\mathfrak{H}}[u(\sigma;\, U)]^n \to \mathrm{pr}_{\mathfrak{H}} E(\sigma) = B(\sigma).$$

Or on a, par le calcul fonctionnel développé dans l'article [5],

$$\mathrm{pr}_{\mathfrak{H}}[u(\sigma;\, U)]^n = [u(\sigma;\, T)]^n,$$

donc

$$[u(\sigma;\, T)]^n \to B(\sigma),$$

ce qui entraîne que $[B(\sigma)]^2 = \lim [u(\sigma;\, T)]^{2n} = B(\sigma)$. Comme de plus $B(\sigma)$ est une transformation autoadjointe de l'espace $\mathfrak{H}$, il résulte que $B(\sigma)$ est une projection orthogonale de $\mathfrak{H}$ sur un certain sous-espace $\mathfrak{H}(\sigma) \subseteq \mathfrak{H}$. $\mathfrak{H}(\sigma)$ réduit T puisque, en vertu de la propriété multiplicative de calcul fonctionnel mentionné, on a

$$T[u(\sigma;\, T)]^n = [u(\sigma;\, T)]^n T,$$

ce qui donne à la limite $(n \to \infty)$:

$$TB(\sigma) = B(\sigma) T.$$

En désignant par σ_θ la partie de l'ensemble σ située dans l'intervalle $[0, \theta]$, σ_0 sera aussi un ensemble fermé et de mesure $m(\sigma_0) = 0$, donc $B(\sigma_0) = \mathrm{pr}_{\mathfrak{H}} E(\sigma_\theta)$ sera par la même raison une projection orthogonale de $\mathfrak{H}$ sur un sous-espace de $\mathfrak{H}$. Il résulte de la relation $E(\sigma_\theta) = E(\sigma) E_\theta = E_\theta E(\sigma)$ que $E(\sigma_0)$ est une fonction non-drécroissante de θ dans l'intervalle $0 \leqq \theta \leqq 2\pi$, continue de droite et telle que $E(\sigma_0) = O$, $E(\sigma_{2\pi}) = E(\sigma)$. Ces propriétés de $E(\sigma_0)$ se transmettent aussi à $B(\sigma_0)$, donc, considéré dans $\mathfrak{H}(\sigma)$, $\{B(\sigma_\theta)\}$ est une famille spectrale et par conséquent

$$\int_0^{2\pi} e^{i\theta}\, d_\theta B(\sigma_\theta)$$

est une transformation unitaire. Or cette transformation unitaire de $\mathfrak{H}(\sigma)$ est égale à la partie de T dans $\mathfrak{H}(\sigma)$; en effet on a pour $h \in \mathfrak{H}(\sigma)$:

$$Th = PUh = \int_0^{2\pi} e^{i\theta}\, dP E_\theta E(\sigma) h = \int_0^{2\pi} e^{i\theta}\, dP E(\sigma_\theta) h = \int_0^{2\pi} e^{i\theta}\, dB(\sigma_\theta) h.$$

La partie de T dans $\mathfrak{H}(\sigma)$ est donc unitaire. Comme T était supposée complètement non-unitaire, on a nécessairement $\mathfrak{H}(\sigma) = (0)$, donc $B(\sigma) = O$ ou, ce qui ce qui revient au même, $PE(\sigma)P = O$ (dans $\mathfrak{K}$). Cela entraîne que $E(\sigma)P = O$ (parce que $[E(\sigma)P]^* E(\sigma)P = PE(\sigma)P = O$). Comme $E(\sigma)$ et U permutent, on a donc pour tout $h \in \mathfrak{H}$ et tout entier n

$$E(\sigma) U^n h = E(\sigma) U^n P h = U^n E(\sigma) P h = 0.$$

Vu que les éléments de la forme $U^n h$ ($h \in \mathfrak{H}$, n entier) sous-tendent l'espace $\mathfrak{K}$, on en conclut que $E(\sigma) = O$.

Ainsi on a démontré que pour tout ensemble fermé σ de mesure $m(\sigma) = 0$ on a $E(\sigma) = O$.

Il s'ensuit que pour tout $f \in \mathfrak{K}$ la fonction $(E_\theta f, f)$ est absolument continue. En effet, cette fonction non-décroissante engendre la mesure de Lebesgue—Stieltjes $m_f(\sigma) = (E(\sigma)f, f)$ pour les ensembles boréliens σ, donc ce qu'il faut montrer c'est que $m(\sigma) = 0$ entraîne $m_f(\sigma) = 0$. En cas contraire il y aurait un ensemble borélien σ et un $f \in \mathfrak{K}$ tels que $m(\sigma) = 0$, $m_f(\sigma) > 0$, et alors — en vertu de la régularité de la mesure de Lebesgue—Stieltjes — il y aurait aussi un ensemble *fermé* $\sigma' (\subseteq \sigma)$ pour lequel $m(\sigma') = 0$ et $m_f(\sigma') > 0$, ce qui contredit à ce que $E(\sigma') = O$.

Le reste de la démonstration est un raisonnement usuel dans la théorie de la multiplicité spectrale. On choisit dans $\mathfrak{K}$ un ensemble $\{f_\omega\}_{\omega \in \Omega}$ d'éléments $\neq 0$ tels que

$$\mathfrak{K} = \bigoplus_{\omega \in \Omega} \mathfrak{M}_\omega,$$

$\mathfrak{M}_\omega$ désignant le sous-espace de $\mathfrak{K}$ sous-tendu par les éléments $U^n f_\omega$ ($n = 0, \pm 1, \pm 2, \ldots$). Ces sous-espaces réduisent U et en désignant par U_ω la partie de U dans $\mathfrak{M}_\omega$ on a $U = \bigoplus_{\omega \in \Omega} U_\omega$. Soit $\mathfrak{M}_\omega^0$ l'ensemble linéaire, partout dense dans $\mathfrak{M}_\omega$, formé par les sommes finies de la forme

$$\sum_n c_n U^n f_\omega.$$

De la relation

$$(U^n f_\omega, U^m f_\omega) = (U^{n-m} f_\omega, f_\omega) = \int_0^{2\pi} e^{i(n-m)\theta} d(E_\theta f_\omega, f_\omega)$$

il s'ensuit, en posant

$$p_\omega(\theta) = \sqrt{d(E_\theta f_\omega, f_\omega)/d\theta}$$

et en désignant par M_ω l'ensemble des points θ où $p_\omega(\theta)$ existe et est $\neq 0$, que l'application

$$f = \sum_n c_n U^n f_\omega \to \sum_n c_n e^{in\theta} p_\omega(\theta) = f(\theta)$$

de $\mathfrak{M}_\omega^0$ dans $L^2(M_\omega)$ est linéaire et isométrique, de plus telle que

$$Uf \to e^{i\theta} f(\theta). \tag{3}$$

Il est aisé de voir que les fonctions ainsi obtenues $f(\theta)$ sont partout denses dans $L^2(M_\omega)$, donc l'application envisagée s'étend par continuité à une application linéaire et isométrique de $\mathfrak{M}_\omega$ *sur* $L^2(M_\omega)$; la correspondance (3)

subsistera aussi après ce prolongement. Cela prouve que U_ω est unitairement équivalente à la multiplication par $e^{i\theta}$ dans $L^2(M_\omega)$.

Théorème 2 est ainsi complètement démontré.

Remarquons encore que les espaces $L^2(M_\omega)$ étant de dimension $\mathfrak{a}$ (puissance d'un ensemble dénombrablement infini) on a $\operatorname{Dim}\mathfrak{K} = \mathfrak{a}\cdot\mathfrak{i}$ où $\mathfrak{i}$ est la puissance de l'ensemble des indices Ω. Comme d'autre part $\operatorname{Dim}\mathfrak{K} \leqq \mathfrak{a}\cdot\operatorname{Dim}\mathfrak{H}$, il s'ensuit que $\mathfrak{a}\cdot\mathfrak{i} \leqq \mathfrak{a}\cdot\operatorname{Dim}\mathfrak{H}$, donc

$$\mathfrak{i} \leqq \mathfrak{a}\cdot\operatorname{Dim}\mathfrak{H}. \tag{4}$$

Vu que chaque espace $L^2(M_\omega)$ peut être considéré comme un sous-espace de l'espace $L^2(0, 2\pi)$ et que $V(M_\omega) \oplus V(CM_\omega) = V(0, 2\pi)$, la dilatation unitaire U peut être prolongée, dans un certain espace $\mathfrak{K}'$, à une transformation unitaire U' qui est la somme orthogonale de $\mathfrak{i}$ répliques de l'opérateur de multiplication par $e^{i\theta}$ des fonctions $f(\theta) \in L^2(0, 2\pi)$. En augmentant au besoin le nombre de ces répliques on peut même supposer (tenant compte de (4)) que leur nombre total est égal au nombre cardinal

$$\mathfrak{i}' = \mathfrak{a}\cdot\operatorname{Dim}\mathfrak{H},$$

c'est-à-dire que $\mathfrak{i}' = \mathfrak{a}$ si $\mathfrak{H}$ est séparable et $\mathfrak{i}' = \operatorname{Dim}\mathfrak{H}$ si $\mathfrak{H}$ est non séparable. La transformation unitaire U' obtenue vérifiera les conditions $T^n = \operatorname{pr}_{\mathfrak{H}} U'^n$ $(n = 0, 1, 2, \ldots)$ mais en général $\mathfrak{K}'$ ne sera plus déterminé par les éléments de la forme $U'^n h$ $(h \in \mathfrak{H};\ n = 0, \pm 1, \pm 2, \ldots)$.

2. Cas d'un semi-groupe à un paramètre de contractions

Passons à l'étude analogue d'un semi-groupe continu $\{T_s\}_{s \geqq 0}$ de contractions de $\mathfrak{H}$ et sa dilatation unitaire $\{U_s\}_{-\infty < s < \infty}$ qui est un groupe continu à un paramètre de transformations unitaires d'un certain espace $\mathfrak{K} \supseteq \mathfrak{H}$, tel que

$$T_s = \operatorname{pr}_{\mathfrak{H}} U_s \qquad (s \geqq 0)$$

et $\mathfrak{K}$ est sous-tendu par les éléments de la forme $U_s h$ $(h \in \mathfrak{H};\ s$ réel); la structure $\{\mathfrak{K}, U_s, \mathfrak{H}\}$ est alors déterminée à isomorphie près [6]).

La dilatation unitaire d'une somme orthogonale $\bigoplus_\omega T_s^{(\omega)}$ de semi-groupes continus de contraction est évidemment égale à la somme orthogonale $\bigoplus_\omega U_s^{(\omega)}$ des dilatations unitaires correspondantes.

Un semi-groupe $\{T_s\}$ de transformations linéaires bornées de $\mathfrak{H}$ sera dit *complètement non-unitaire* si pour tout $h \in \mathfrak{H}$, $h \neq 0$, au moins une des fonctions $\|T_s h\|, \|T_s^* h\|$ de s $(0 \leqq s < \infty)$ n'est pas constamment égale à $\|h\|$.

[6]) Cf. [2—5].

Théorème 3. *A tout semi-groupe continu* $\{T_s\}_{s\geqq 0}$ *de l'espace* $\mathfrak{H}$ *correspond une décomposition de* $\mathfrak{H}$ *en somme orthogonale des deux sous-espaces orthogonaux complémentaires* $\mathfrak{H}^{(u)}$ *et* $\mathfrak{H}^{(0)}$ [7]) *réduisant les transformations* T_s *et tels que les parties de* T_s *dans* $\mathfrak{H}^{(u)}$ *et* $\mathfrak{H}^{(0)}$ *forment, selon les cas, un semi-groupe unitaire* $\{T_s^{(u)}\}$ *et un semi-groupe complètement non-unitaire* $\{T_s^{(0)}\}$. *Cette décomposition est unique,* $\mathfrak{H}^{(u)}$ *étant constitué des éléments* h *pour lesquels*

$$\|T_s h\| = \|h\| = \|T_s^* h\| \quad \textit{pour tout} \quad s \geqq 0. \tag{5}$$

$\{T_s^{(u)}\}$ et $\{T_s^{(0)}\}$ seront appelés la *partie unitaire* et la *partie complètement non-unitaire* du semi-groupe $\{T_s\}$.

Démonstration. Faisant intervenir la dilatation unitaire $\{U_s\}_{-\infty<s<\infty}$ de $\{T_s\}_{s\geqq 0}$ on montre d'abord que l'ensemble $\mathfrak{H}^{(u)}$ des éléments $h \in \mathfrak{H}$ vérifiant (5) peut être représenté sous la forme

$$\mathfrak{H}^{(u)} = \bigcap_{-\infty<s} \; \bigcap_{\infty} U_{-s}\mathfrak{H},$$

ce qui met en évidence que cet ensemble est un sous-espace de $\mathfrak{H}$, appliqué par chaque U_t sur lui-même. On achève la démonstration tout comme celle du théorème 1.

Comme un corollaire du théorème 3 on peut affirmer que la dilatation unitaire $\{U_s\}$ de $\{T_s\}$ est égale à la somme orthogonale de $\{T_s^{(u)}\}$ et de la dilatation unitaire $\{U_s^{(0)}\}$ de $\{T_s^{(0)}\}$. Cela impose le problème d'étudier de plus près les dilatations unitaires des semi-groupes de contractions complètement non-unitaires. Cette étude peut être réduite au cas envisagé dans le théorème 2 si l'on fait intervenir les *cogénératices* des semi-groupes en question [8]).

Lemme. *La décomposition de l'espace* $\mathfrak{H}$ *qui correspond au semi-groupe continu de contractions* $\{T_s\}$, *au sens du théorème 3, est la même que celle qui correspond à la cogénératrice* T *de ce semi-groupe, au sens du théorème 1.*

Démonstration. Soit $\mathfrak{H} = \mathfrak{H}^{(u)} \oplus \mathfrak{H}^{(0)}$ la décomposition correspondant à $\{T_s\}$ au sens du théorème 3, et soient T, T', T'' les cogénératrices des semi-groupes $\{T_s\}$, $\{T_s^{(u)}\}$, $\{T_s^{(0)}\}$; ces sont des contractions dans les espaces $\mathfrak{H}$, $\mathfrak{H}^{(u)}$, $\mathfrak{H}^{(0)}$, selon les cas, et on a évidemment $T = T' \oplus T''$. T est unitaire puisque le semi-groupe $\{T_s\}$ est unitaire (cf. [5], th. 4); montrons que T'' est complètement non-unitaire. En effet, si T'' avait la partie unitaire $T''^{(u)}$ non banale, c'est-à-dire définie dans un sous-espace $\mathfrak{H}^{(1)}$ de $\mathfrak{H}^{(0)}$ constitué non seulement de l'élément 0, alors $\mathfrak{H}^{(1)}$ réduirait aussi le semi-groupe $\{T_s^{(0)}\}$, et la partie de $\{T_s^{(0)}\}$ dans $\mathfrak{H}^{(1)}$, ayant sa cogénératrice $T''^{(u)}$ unitaire, serait

[7]) $\mathfrak{H}^{(u)}$ ou $\mathfrak{H}^{(0)}$ peut se réduire au seul élément 0.

[8]) Cf. [5], chap. II.

lui-même unitaire (cf. [5], th. 4), ce qui contredit à ce que $\{T_s^{(\prime)}\}$ est un semi-groupe complètement non-unitaire. Par conséquent T' et T'' coïncident avec les parties unitaire et complètement non-unitaire de T, c. q. f. d.

Envisageons alors un groupe continu de contractions $\{T_s\}$ dans l'espace $\mathfrak{H}$, complètement non-unitaire. Soit $\{U_s\}$ la dilatation unitaire de $\{T_s\}$ dans un certain espace $\mathfrak{K} \supseteq \mathfrak{H}$. Soient T et U les cogénératrices correspondantes. D'après le lemme, T est une contraction complètement non-unitaire de $\mathfrak{H}$, tandis que U est une transformation unitaire de $\mathfrak{K}$ (cf. [5], th. 4). En vertu de la relation

$$U_s = \exp[s(U+1)(U-1)^{-1}]$$

entre le semi-groupe unitaire $\{U_s\}$ et sa cogénératrice U (cf. [5], p. 35—36) les familles spectrales $\{E_\theta\}$ $(0 \leqq \theta \leqq 2\pi)$ et $\{F_x\}$ $(-\infty < x < \infty)$ correspondant à U et à U_s par les formules

$$U = \int_0^{2\pi} e^{i\theta} dE_\theta \quad \text{et} \quad U_s = \int_{-\infty}^{\infty} e^{isx} dF_x \text{ [9])}$$

sont liées l'une à l'autre par la relation

$$F_x = E_{2 \operatorname{arc\,tg} x} \qquad (-\infty < x < \infty).$$

Or, d'après un théorème général (cf. [5], th. 5) la cogénératrice U de $\{U_s\}$ est égale à la dilatation unitaire de la cogénératrice T de $\{T_s\}$. Donc U est la dilatation unitaire d'une contraction complètement non-unitaire, d'où il résulte en appliquant le théorème 2:

Théorème 4. *La dilatation unitaire $\{U_s\}$ d'un semi-groupe à un paramètre de contractions $\{T_s\}$, complètement non-unitaire, a son spectre absolument continu. D'une manière plus précise, $\{U_s\}$ est unitairement équivalent à une somme orthogonale de type $\bigoplus_{\omega \in \Omega} \{V_s(M_\omega)\}$, où $V_s(M_\omega)$ désigne la multiplication par e^{isx} dans l'espace $L^2(M_\omega)$ des fonctions $f(x)$ définies dans un ensemble mesurable $M_\omega \subseteq (-\infty, \infty)$.*

Des remarques additionnelles, analogues à celles faites à la fin du paragraphe précédent, s'appliquent aussi dans ce cas.

[9]) On y ajoute la condition de continuité de droite de E_θ et que $E_0 = O$.

Ouvrages cités

[1] F. et M. Riesz, Über die Randwerte einer analytischen Funktion, *Quatrième Congrès des math. scandinaves*, **1956**, 27—44.

[2] B. Sz-Nagy, *Prolongements des transformations de l'espace de Hilbert qui sortent de cet espace.* Appendice au livre "Leçons d'analyse fonctionnelle" par F. Riesz et B. Sz.-Nagy (Budapest, 1955).

[3] ——— Sur les contractions de l'espace de Hilbert, *Acta Sci. Math.*, **15** (1953), 87—92.

[4] ——— Sur les contractions de l'espace de Hilbert. II, *ibidem*, **18** (1957), 1—15.

[5] ——— et C. Foiaş, Sur les contractions de l'espace de Hilbert. III, *ibidem*, **19** (1958) 26—45.

(Reçu le 26 février 1960)

On independent sets of elements in algebra*)

By A. KERTÉSZ in Debrecen

To Professor L. Rédei on his 60th birthday

§ 1. Introduction

In connection with the different concepts of "independence" which arise in the investigation of different algebraic structures, there are known theorems which assert that maximal independent sets of elements must have the same cardinality. Making use of what is really a generalization of the essence of STEINITZ's exchange theorem, we give in the present note a method which can advantageously be employed in proving theorems of this type (Theorem 1). Some applications of Theorem 1 are found in § 3. There in particular we determine the class of all those associative rings R for which any two maximal independent systems of elements of any torsion free R-module have the same cardinal number.

§ 2. Abstract dependence

Let S be an arbitrary set and $D[x, A]$ a binary relation defined between elements x and subsets A of S, satisfying the following conditions:

(I) If $x \in A$, then $D[x, A]$.

(II) If $D[x, A]$, $a \in A$ and $\bar{D}[x, A \setminus \{a\}]$, then $D[a, (A \setminus \{a\}) \cup \{x\}]$.[1])

(III) If $D[x, A]$ and $D[a, B]$ for all elements $a \in A$, then $D[x, B]$.

(IV) If $D[x, A]$, then there exists a finite subset A' of A such that $D[x, A']$.

If $D[x, A]$ holds, we say that x *depends on* A. We say that *the set* $A(\subseteq S)$, *depends on the set* $B(\subseteq S)$, if each element of A depends on B,

*) This paper was presented at a scientific session at Debrecen University in April 1959.

[1]) By $\bar{D}[x, B]$ we denote the fact that the relation $D[x, B]$ is not valid. In the case of two sets A and B, $A \setminus B$ denotes the set of those elements of A which are not contained in B. The empty set is denoted by $\emptyset$, and the cardinal number of A is $|A|$.

and in this case we write $D[A, B]$. If $D[A, B]$ and $D[B, A]$ both hold, then A and B are said to be *D-equivalent*. A set $A(\subseteq S)$ is said to be *D-dependent*, if there exists an element a in A such that $D[a, A \setminus \{a\}]$. In the contrary case A is said to be *D-independent*. On the basis of (IV) it is clear that a set A is D-independent if and only if each of its finite subsets is D-independent.

If we suppose that in the relation $D[x, A]$ the set A is always finite, then the properties (I'), (II'), (III') corresponding in this special case to (I), (II) and (III) are exactly the well known axioms of abstract dependence. It is also known that (I'), (II') and (III') imply that *two finite independent equivalent sets have the same number of elements.*[2]) With the aid of (I)—(IV) we are now going to prove this theorem in the general case. It is possible to give a proof which reduces the problem to the finite case;[3]) we give here, however, a direct proof in which the finite case plays no distinguished role.

Theorem 1. *Let $D[x, A]$ be a relation defined on a set S and satisfying the conditions* (I)—(IV). *Then any two D-equivalent D-independent subsets of S have the same cardinal number.*[4])

Proof. Let $H(\subseteq S)$ and $K(\subseteq S)$ be two D-equivalent D-independent sets. Owing to symmetry it will be sufficient to show that if $|H| = \mathfrak{m}$, then $|K| \geqq \mathfrak{m}$.

Let the symbol

$$(H', K', \varphi') \tag{1}$$

express the fact that φ' is a one-to-one mapping of the set $H'(\subseteq H)$ onto the set $K'(\subseteq K)$, and that the set $R' = K' \cup (H \setminus H')$ is D-independent. We denote by Q the set of all triplets (1). This set is certainly non-empty, since we allow also the possibility of H', K' being empty sets and φ' the empty mapping. Q can be turned into a partially ordered set by agreeing that for two different triplets (H', K', φ') and (H'', K'', φ'')[5]) the relation $(H', K', \varphi') < (H'', K'', \varphi'')$ holds if and only if $H' \subset H''$, $K' \subset K''$ and φ'' is a continuation of φ'. We show that the set Q is inductive, i. e. each ordered subset

$$\cdots < (H', K', \varphi') < (H'', K'', \varphi'') < \cdots \tag{2}$$

---

[2]) See e. g. VAN DER WAERDEN [11], § 36, and PICKERT [8].

[3]) In this connection we refer to the method employed in [5].

[4]) The author had access to a paper by M. N. BLEICHER and G. B. PRESTON on "Abstract linear dependence relations" awaiting publication in *Publicationes Mathematicae Debrecen.* This theorem is also proved there, but on quite different lines.

[5]) Two triplets (H', K', φ'), (H'', K'', φ'') are to be considered different if at least one of the relations $H' \neq H''$, $K' \neq K''$ and $\varphi' \neq \varphi''$ holds.

of Q has an upper bound in Q. We indeed have

$$\cdots \subset H' \subset H'' \subset \cdots ; \quad \cdots \subset K' \subset K'' \subset \cdots .$$

Let us consider the subsets

$$H_0 = \cdots \cup H' \cup H'' \cup \cdots \ (\subseteq H) \qquad \text{and} \qquad K_0 = \cdots \cup K' \cup K'' \cup \cdots \ (\subseteq K).$$

First we remark that $R_0 = K_0 \cup (H \setminus H_0)$ is D-independent, since any finite subset of R_0 is contained in a suitable set of the form $R' = K' \cup (H \setminus H')$, and such a set is D-independent. Moreover it is clear that there exists a one to one mapping φ_0 of H_0 onto K_0 which is a continuation of each of the mappings φ in (2). So (H_0, K_0, φ_0) is an upper bound of (2).

Thus by the lemma of KURATOWSKI—ZORN Q has a maximal element (H^*, K^*, φ^*). We show that $H = H^*$. If this is true, then $R^* = K^* \cup (H \setminus H^*) = K^* \subseteq K$; in view of the equal cardinality of H^* and K^* the set R^* has cardinality $\mathfrak{m}$, so that $|K| \geqq \mathfrak{m}$.

Suppose our assertion to be false, i.e. $H^* \subset H$. First note that in this case H has an element h which is also an element of R^*, and K has an element k for which $\overline{D}[k, R^* \setminus \{h\}]$ holds and so, by (1), $k \notin K^*$. For if we had $D[K, R^* \setminus \{h\}]$, then by $D[h, K]$ and (III) the relation $D[h, R^* \setminus \{h\}]$ would also hold, contradicting the D-independence of R^*. Secondly, the set $R^{**} = (R^* \setminus \{h\}) \cup \{k\}$ is D-independent. Otherwise there would exist an element $r (\in R^{**})$ for which $D[r, R^{**} \setminus \{r\}]$: if $r = k$, then we have at once $D[k, R^* \setminus \{h\}]$, a contradiction; if $r \neq k$, then with the help of $\overline{D}[r, R^{**} \setminus \{r, k\}]$ and (II) we again have $D[k, R^* \setminus \{h\}]$. Finally denoting by φ^{**} the mapping of $H^* \cup \{h\}$ onto $K^* \cup \{k\}$ which arises if we complete the mapping φ^* of H^* onto K^* by the mapping $h \to k$, we get

$$(H^*, K^*, \varphi^*) < (H^* \cup \{h\}, K^* \cup \{k\}, \varphi^{**}),$$

which contradicts the maximality of (H^*, K^*, φ^*). This completes the proof of Theorem 1.

We remark that since by (IV) the D-independence defined above is a property of finite character, according to the lemma of TEICHMÜLLER—TUKEY the set S has a maximal D-independent subset. It is also clear that two maximal D-independent subsets are equivalent, and this gives us the following corollary to our theorem:

Corollary. *Any two maximal D-independent subsets of the set S have the same cardinality.*

§ 3. Applications

1. Let M be an arbitrary set. Following WHITNEY [12], we define a *rank function* r on M which associates with every finite subset A of M a non-negative integer $r(A)$ satisfying the axioms (R_1), (R_2), (R_3) as follows:

(R_1) $r(\emptyset)=0$,

(R_2) $r(A\cup\{x\})=r(A)+k$, where $k=0$ or 1,

(R_3) if $r(A)=r(A\cup\{x\})=r(A\cup\{y\})$ then $r(A)=r(A\cup\{x,y\})$.

A finite set $A(\subseteq M)$ is said to be *r-independent* if $r(A)=|A|$. We say that the arbitrary set $A(\subseteq M)$ is r-independent if each of its finite subsets is r-independent.

As a first application of Theorem 1 we prove the following theorem of R. RADO [9]:

Any two maximal r-independent subsets of the set M have the same cardinality.

Let us be given on the set M the function $r(A)$. We define on M a relation $D[x, A]$ in the following way: $D[x, A]$ is to be valid if and only if there exists a finite subset A' of A such that $r(A'\cup\{x\})=r(A')$. In view of the evident fact that on M the concepts of r-independence and D-independence coincide, in order to prove the theorem of RADO with the aid of the Corollary of Theorem 1, it will be sufficient to show that for the relation $D[x, A]$ conditions (I)—(IV) are satisfied.

It is clear that (I) and (IV) hold. Suppose now $D[x, A]$, $a\in A$ and $\overline{D}[x, A\setminus\{a\}]$ to be valid. Then A has a finite subset A' for which

$$r(A')=r(A'\cup\{x\}), \tag{3}$$

$$r(A'\setminus\{a\})<r((A'\setminus\{a\})\cup\{x\}) \tag{4}$$

hold. On the basis of (R_2) we obtain from (4) with the aid of (3)

$$r(A')\leqq r((A'\setminus\{a\})\cup\{x\})\leqq r(A'\cup\{x\})=r(A')$$

and consequently

$$r((A'\setminus\{a\})\cup\{x\})=r('\cup A\{x\})$$

which shows $D[a, (A'\setminus\{a\})\cup\{x\}]$ to be true, proving so the validity of (II).

In order to show that (III) is also valid, we shall need two simple lemmas:

L e m m a 1. *If* $r(A)=r(A\cup\{x_1\})=\cdots=r(A\cup(x_n\})$, *then* $r(A)=$ $=r(A\cup\{x_1,\ldots,x_n\})$.

Our assertion is true for $n=2$ by (R_3). We suppose it to be valid for $n-1$. Then $r(A)=r(A\cup\{x_1,\ldots,x_{n-2},x_{n-1}\})=r(A\cup\{x_1,\ldots,x_{n-2},x_n\})$. Making use again of (R_3) we get $r(A)=r(A\cup\{x_1,\ldots,x_n\})$.

Lemma 2. *If* $r(A) = r(A \cup \{x\})$, *then for any finite set* Y *the relation* $r(A \cup Y) = r(A \cup Y \cup \{x\})$ *holds.*

It will clearly be sufficient to prove our assertion for the case $Y = \{y\}$. If $r(A \cup \{y\}) = r(A)$, then $r(A) = r(A \cup \{x\})$ and by (R_3) $r(A \cup \{y\}) = r(A \cup \{x, y\})$. On the other hand if $r(A \cup \{y\}) = r(A) + 1$, then by $r(A \cup \{x, y\}) \geqq r(A \cup \{y\}) \geqq r(A) = r(A \cup \{x\})$ and by (R_2) $r(A \cup \{x, y\}) = r(A) + 1$, i. e. $r(A \cup \{y\}) = r(A \cup \{x, y\})$ also holds.

Suppose now $D[x, A]$ and $D[a, B]$ to be valid for any element $a \in A$. We show that in this case $D[x, B]$ also holds. Without prejudice to generality we may suppose that $A = \{a_1, \ldots, a_n\}$ and B are finite. Since by our hypotheses and Lemma 2 $r(A) = r(B \cup a_i)$ for $i = 1, \ldots, n$, in view of Lemma 1 we get

$$r(B) = r(A \cup B). \tag{5}$$

On the other hand, by virtue of $r(B \cup \{a_1\}) = r(B)$ and of Lemma 2 we obtain

$$r(B \cup \{a_1, x\}) = r(B \cup \{x\}), \tag{6}$$

and by virtue of $r(B \cup \{a_2\}) = r(B)$ and of Lemma 2

$$r(B \cup \{a_1, a_2, x\}) = r(B \cup \{a_1, x\}). \tag{7}$$

From (6) and from (7) there follows

$$r(B \cup \{a_1, a_2, x\}) = r(B \cup \{x\}).$$

A continuation of this procedure yields in the n-th step

$$r(B \cup A \cup \{x\}) = r(B \cup \{x\}). \tag{8}$$

Finally from $r(A) = r(A \cup \{x\})$ we get on the basis of Lemma 2

$$r(A \cup B) = r(A \cup B \cup \{x\}) \tag{9}$$

and so by (5), (9) and (8)

$$r(B) = r(B \cup \{x\}),$$

i. e. $D[x, B]$ is valid. This proves (III).[6])

Making now use of the Corollary of Theorem 1, we can complete the proof of RADO's theorem.

2. Let L be an extension of the field K and let x and A be an element and a subset of L respectively. We define the relation $D[x, A]$ in the following way: $D[x, A]$ is to be valid if and only if x is algebraic over $K(A)$.

[6]) We remark that the two sets of axioms (I), (II), (III), (IV) and (R_1), (R_2), (R_3) are in fact equivalent. Indeed, if for the relation $D[x, A]$ defined on the set M conditions (I)—(IV) hold, then let $r(A)$ denote the number of elements of some maximal independent subset of the finite set $A (\subseteq M)$. By virtue of Theorem 1 $r(A)$ is uniquely determined, and it clearly satisfies (R_1)—(R_3).

If $D[x, A]$ holds, we say that x depends algebraically on A. The algebraic independence of a set and the algebraic equivalence of two sets are defined on the basis of $D[x, A]$ as the corresponding D-concepts in § 2.

It is a well-known fact that algebraic dependence has the properties (I)—(IV). So from Theorem 1 we immediately obtain the following theorem of STEINITZ [10]:

Let L be an extension of the field K and let A and B be two subsets of L, algebraically independent and equivalent (over K). Then A and B have the same cardinal number.

3. We call an element x of the group G a distinguished element, if it generates a minimal normal subgroup in G. Let us consider the set S of all distinguished elements of G, and let us define on this set the relation $D[x, A]$ in the following manner: $D[x, A]$ is to be valid if and only if $x(\in S)$ is an element of the normal subgroup generated by $A(\subseteq S)$. It is evident that (I), (III) and (IV) are fulfilled. The validity of (II) can also be shown without difficulty. Let $D[x, A]$ and $D[x, A \setminus \{a\}]$, $a \in A$ hold. Then a relation of the form $x = bc$ holds, where c is an element, different from 1, of the normal subgroup generated by the element a, and b is an element of a normal subgroup generated by a finite subset of A not containing the element a. Hence we obtain $b^{-1}x = c(\neq 1)$, and since the normal subgroup generated by c contains, in view of the distinguishedness of a, the element a, a is in fact an element of the normal subgroup generated by $(A \setminus \{a\}) \cup \{x\}$, so that $D[a, (A \setminus \{a\}) \cup \{x\}]$. If we define independence in an analogous manner as in § 2, we can infer from Theorem 1 that two maximal independent subsets of the set of all distinguished elements of G have the same cardinal number.

In view of this fact, it is not hard to establish the following

Theorem 2. *Let G be a group which is decomposable into the direct product of simple groups. If $G = \prod_{\mu \in \Gamma} H_\mu$ and $G = \prod_{\nu \in \Delta} K_\nu$ are two such decompositions of G, then Γ and Δ have the same cardinal number.*

To complete the proof, let us take from each direct factor H_μ and K_ν exactly one element $h_\mu(\neq 1)$ and $k_\nu(\neq 1)$ respectively. Then the sets $\{h_\mu\}_{\mu \in \Gamma}$ and $\{k_\nu\}_{\nu \in \Delta}$ are maximal independent subsets of the set of distinguished elements of G, having thus equal cardinality on the basis of our above results.

In the same manner we can obtain an analogous result for the case of rings (modules) decomposable into the direct sum of simple rings (irreducible modules). For modules this result is already known (see [2], p. 62 and [3]). The theorem on modules clearly comprises also the theorem on the dimension of a vector space over a skewfield.

4. Any two maximal independent systems of elements of a torsion-free abelian group have the same cardinal number (see, for instance, [6] or [1]). However, this result does not carry over to modules with an arbitrary domain of operators. As a further application of Theorem 1 we determine the class of all rings R which are such that the result just mentioned holds for every torsion-free R-module.[7])

This problem can be considered in two different ways. Module theory is often restricted to the case where R has a unit element which acts as identity operator; then we talk about unitary R-modules. The order of an element g of a unitary R-module G is the set of all r ($\in R$) such that $rg=0$. G is torsion-free if all its nonzero elements are of order zero. The element g is dependent on the subset A of G if, for some r ($\in R$), $rg \neq 0$ and rg belongs to the submodule generated by A; independence is defined accordingly, as in § 2.[8]) — On the other hand, in a general approach to module theory no restrictions are necessary: every R-module is considered as a unitary R^*-module in a natural way, and order, dependence, etc., are then defined in terms of R^*.[9]) Note that most statements on a module depend on whether it is considered as a unitary R-module (if it can be considered as such) or just as an R-module (in the general sense).

In both cases the solution of the problem leads essentially to the class of regular rings in the sense of O. Ore [7]. There a ring R is called *regular* if it has no zero divisors and if, for every two nonzero elements a, b of R, the equation $xa+yb=0$ has a nontrivial solution in R. We shall also use the following equivalent definition: R is regular if it has no zero divisors and if any two nonzero left ideals of R have nonzero intersection.

---

[7]) An R-module G is an (additive) abelian group with the (associative) ring R as a left operator domain.

[8]) It follows immediately that an arbitrary set of nonzero elements $g_1, g_2, \ldots$ of G is independent if and only if for every finite subset of this set a relation

$$r_1 g_{i_1} + \cdots + r_n g_{i_n} = 0 \qquad (r_j \in R;\ j = 1, \ldots, n)$$

always implies

$$r_1 g_{i_1} = \cdots = r_n g_{i_n} = 0.$$

If G is torsion-free, then the latter equalities imply $r_1 = \ldots = r_n = 0$.

[9]) See [4]. In particular, R^* is the Dorroh-extension of R by a formal unit element. A set of nonzero elements $g_1, g_2, \ldots$ of G is independent in this sense if for every finite subset of this set a relation

$$\langle r_1, n_1 \rangle g_{i_1} + \cdots + \langle r_k, n_k \rangle g_{i_k} = 0$$

always implies

$$\langle r_1, n_1 \rangle g_{i_1} = \cdots = \langle r_k, n_k \rangle g_{i_k} = 0.$$

If G is torsion-free, then the latter equalities imply $\langle r_1, n_1 \rangle = \ldots = \langle r_k, n_k \rangle = \langle 0, 0 \rangle$. For the notation $\langle r_j, n_j \rangle$ see also [4].

Theorem 3. *Let R be a ring with unit element* 1. *In order that*

(A) *any two maximal independent systems of elements of any torsion-free unitary R-module have the same cardinal number, it is necessary and sufficient that one of the following conditions hold:*

(a) *R has zero divisors;*

(b) *R is regular.*

Theorem 4. *Let R be any ring. In order that*

(B) *any two maximal independent systems of elements of any torsion-free R-module have the same cardinal number, it is necessary and sufficient that one of the following conditions hold:*

(a) *R has zero divisors;*

(a′) *R has nonzero elements of finite additive order;*

(a″) *R contains a nontrivial subring isomorphic to a subring of the rational integers;*

(b) *R is regular.*

Proof of Theorem 3. Suppose first that (A) holds and that R has no divisors of zero. Then R considered as a unitary R-module is torsion-free, and has 1 as a maximal independent system of elements. By virtue of (A) any two nonzero elements a, b of R are not independent, and consequently the equation $xa+yb=0$ admits a nontrivial solution. So R is regular.

Conversely, let (a) or (b) be fulfilled. If R has divisors of zero, then there exist no torsion-free unitary R-modules, and so (A) holds. Let now the ring R be regular. By virtue of Theorem 1, in order to establish the validity of (A), it will be sufficient to show that in the case of torsion-free unitary modules the dependence of an element x on a set A, which from now on we shall denote by $D[x, A]$, has the properties (I)—(IV).

(I), (II) and (IV) are clearly valid. Let G be a torsion-free unitary R-module and let $D[g, U]$, $D[U, V]$ be fulfilled. We show that $D[g, V]$ is also valid. According to (IV) $D[g, U]$ means that, for a suitable finite subset $u_1, \ldots, u_k$ of U, a relation of the form

$$r_0 g = r_1 u_1 + \cdots + r_k u_k \tag{10}$$

holds. In view of $D[U, V]$ and (IV) for suitably chosen elements v_{ij} of V we likewise have the equalities

$$\begin{cases} r_{10} u_1 = r_{11} v_{11} + \cdots + r_{1m_1} v_{1m_1} & (r_{10} \neq 0) \\ \quad \vdots & \\ r_{k0} u_k = r_{k1} v_{k1} + \cdots + r_{km_k} v_{km_k} & (r_{k0} \neq 0). \end{cases} \tag{11}$$

We may suppose that in the equalities (10) and (11) all elements occur-

ring are different from zero. So, by the regularity of R, there exist elements s_α ($\neq 0$) and s'_α ($\neq 0$) ($\alpha = 1, 2, \ldots, k$) of R, for which

$$(12) \qquad \begin{cases} s_1 r_1 u_1 = s'_1 r_{10} u_1 \\ s_2 s_1 r_2 u_2 = s'_2 r_{20} u_2 \\ \vdots \\ s_k \ldots s_2 s_1 r_k u_k = s'_k r_{k0} u_k . \end{cases}$$

Let us now multiply (10) (from the left) by s_1, and the first equation of (11) again from the left by s'_1; by virtue of (12) the element $s_1 r_1 u_1$ can be replaced in the multiplied equation (10) by a linear combination (over R) of the elements v_{ij}. Multiplying the expression so obtained by s_2, and the second equation (11) by s'_2, we effect a further replacement, again on the basis of (12). By a continuation of this process we are able to show finally that the element

$$s_k \ldots s_2 s_1 r_0 g \quad (\neq 0)$$

is contained in the submodule of G generated by the set V, giving $D[g, V]$. This completes the proof of Theorem 3.

Proof of Theorem 4. Let us assume first that (B) holds for R; then (A) holds for R^* and so, according to Theorem 3, either (a) or (b) holds for R^*. If R^* has zero divisors then there can be no torsion-free R-modules. In particular, R itself considered as an R-module is not torsion-free: there is an r ($\in R, r \neq 0$) whose order is a nonzero subring S of R^*. If $S \cap R \neq 0$ then (a) holds for R. If S contains an element of the form $\langle 0, n \rangle$ then R satisfies (a'). If neither of these happens, then there is a one-to-one correspondence between the first and second components of the elements of S, and this is an isomorphism of the kind required for (a''). On the other hand, if R^* is regular then from the second definition of regularity one sees at once that (b) is satisfied by R.

Conversely, if (a) or (a') holds then R^* evidently has zero divisors; and if r ($\neq 0$) corresponds to n in an isomorphism provided by (a''), then $\langle r, -n \rangle \langle r, 0 \rangle = 0$ shows the same. So in these cases there are no torsion-free R-modules. If none of (a), (a'), (a'') holds, then, by what has been said above, R^* cannot have zero divisors. It remains to be shown that in this case (b) implies the regularity of R^*. This will follow if we prove that every nonzero left ideal L of R^* has nonzero intersection with R. But since $rl \in R \cap L$ for every $r \in R$, $l \in L$, it is certainly true (except in the obvious case of $R = 0$). So the application of Theorem 3 completes the proof.

References

[1] L. Fuchs, *Abelian groups* (Budapest, 1958).
[2] N. Jacobson, *Structure of rings* (Providence, 1956).
[3] A. Kertész, Beiträge zur Theorie der Operatormoduln, *Acta Math. Acad. Sci. Hung.*, **8** (1957), 235—257.
[4] A. Kertész, A remark on the general theory of modules, *Publ. Math. Debrecen*, **6** (1959), 86—89.
[5] A. Kertész, Simple proof of a fundamental theorem of field theory, *Amer. Math. Monthly*, **66** (1959), 804.
[6] А. Г. Курош, Теория групп (Москва, 1953).
[7] O. Ore, Linear equations in non-commutative fields, *Ann. of Math.*, **32** (1931), 463—477.
[8] G. Pickert, *Einführung in die Höhere Algebra* (Göttingen, 1951).
[9] R. Rado, Axiomatic treatment of rank in infinite sets, *Canadian Journal of Math.*, **1** (1949), 337—343.
[10] E. Steinitz, *Algebraische Theorie der Körper* (Berlin, 1930).
[11] B. L. van der Waerden, *Moderne Algebra*. I (Berlin—Göttingen—Heidelberg, 1950).
[12] H. Whitney, On the abstract properties of linear dependence, *American Journal of Math.*, **57** (1935), 509—533.

(Received February 29, 1960)

On finite metabelian p-groups with two generators

By G. SZEKERES in Adelaide (South Australia)

To Professor L. Rédei for his 60th birthday

1. The structure problem of finite metabelian groups[1]) is an intricate subject about which only some rather isolated and fragmentary results are known.[2]) At present there is no theory in existence, and probably none in sight, which would give a complete account of all existing (finite) metabelian group structures, e. g. along the lines of the well known theory of finite abelian groups. The diversity of metabelian group structures far exceeds that of ordinary abelian groups and compares with the order of diversity of abelian operator groups over commutative rings of operators. The two types of structures have in fact a great deal in common and the study of abelian operator groups seems to be a necessary prerequisite to any comprehensive theory of metabelian groups.

In the present work we shall be concerned with metabelian p-groups with two generating elements where p is a fixed prime number. The abelian operator groups associated with these groups are cyclic (in the sense that they are generated by a single element) and hence structurally identical with polynomial ideals in one or more variables. We shall make use of this relation to determine all metabelian p-groups with two generators which have a commutator subgroup of type $(p, \ldots, p)$; to remove this last mentioned restriction, it would be necessary to know all polynomial ideals in two variables over the integers (or in three variables over a field) for which there is no satisfactory process of enumeration known at the present time.

Denote by $\mathfrak{A}$ the commutator subgroup of the finite metabelian p-group $\mathfrak{G}$. Let $\mathfrak{G}$ be generated by the elements S, T and $\sigma = S\mathfrak{A}$, $\tau = T\mathfrak{A}$ the corresponding cosets modulo $\mathfrak{A}$. Evidently σ, τ are generating elements of the

[1]) We call a group metabelian if its commutator subgroup is abelian and distinct from the identity. All groups considered in this paper are finite.

[2]) A list of metabelian p-groups with known structure has been compiled at the end of the paper.

(abelian) quotient group $\mathfrak{B} = \mathfrak{G}/\mathfrak{A}$ and we can assume that they are independent basis elements of $\mathfrak{B}$.[3])

Let $\mathfrak{C}$ denote the ring of rational integers and $\mathfrak{C}[\sigma, \tau]$ the (commutative) ring of polynomials in σ, τ with integer coefficients. $\mathfrak{C}[\sigma, \tau]$ is an operator ring for $\mathfrak{A}$ under the well known rules

$$A^{\varrho} = R^{-1} A R, \quad \varrho = \sigma^{k} \tau^{l}, \quad R = S^{h} T^{l}, \tag{1.01}$$

$$A^{\varrho_1 + \varrho_2} = A^{\varrho_1} A^{\varrho_2}, \quad \varrho_1 \in \mathfrak{C}[\sigma, \tau], \quad \varrho_2 \in \mathfrak{C}[\sigma, \tau]. \tag{1.02}$$

As a $\mathfrak{C}[\sigma, \tau]$-group, $\mathfrak{A}$ is cyclic and is generated by the element

$$A_0 = T^{-1} S^{-1} T S. \tag{1.1}$$

In fact, the equations

$$TS = S T A_0 \tag{1.11}$$

$$A_0^{q(\sigma, \tau)} S = S A_0^{\sigma g(\sigma, \tau)} \tag{1.12}$$

$$A_0^{g(\sigma, \tau)} T = T A_0^{\tau g(\sigma, \tau)}, \quad g(\sigma, \tau) \in \mathfrak{C}[\sigma, \tau] \tag{1.13}$$

allow us to reduce every finite product formed by S and T (hence every element of $\mathfrak{G}$) to the form

$$S^{q} T^{r} A_0^{f(\sigma, \tau)} \tag{1.14}$$

where q, r are non-negative integers and $f(\sigma, \tau)$ has non-negative integer coefficients. But the elements $A_0^{f(\sigma, \tau)}$ form a subgroup $\mathfrak{A}^*$ of $\mathfrak{A}$, viz. the $\mathfrak{C}[\sigma, \tau]$-subgroup generated by A_0, and $\mathfrak{G}/\mathfrak{A}^*$ is abelian, as seen from (1.14), so that $\mathfrak{A}^* \supseteq \mathfrak{A}$, whence $\mathfrak{A}^* = \mathfrak{A}$.

Now the set of annulling polynomials $g(u, v)$ for which $A_0^{g(\sigma, \tau)} = 1$[4]) form an ideal $\mathfrak{J}$ in $\mathfrak{C}[u, v]$ with the property that

$$p^{h} \equiv 0 (\mathfrak{J}), \quad u^{p^m} \equiv 1 (\mathfrak{J}), \quad v^{p^n} \equiv 1 (\mathfrak{J}) \tag{1.2}$$

where p^m, p^n are the respective orders of σ, τ and p^h is the exponent of $\mathfrak{A}$. Conversely, given an ideal $\mathfrak{J}$ which satisfies the conditions (1.2) we can construct all groups $\mathfrak{G}$ which belong to this annulling ideal by taking (1.11)—(1.13) as a set of defining relations for $\mathfrak{G}$ and by specifying S^{p^m}, T^{p^n} as suitable elements of $\mathfrak{A}$. It appears therefore that the first step in the determination of these groups is to enumerate (and possibly characterize by numerical invariants) all ideals in $\mathfrak{C}[u, v]$ which satisfy the conditions (1.2).

---

[3]) $\mathfrak{B}$ is evidently non-cyclic.

[4]) We shall use the symbol 1 to denote the identity element of any algebraic system such as groups, fields or operator rings. There is no danger of confusion as it is always clear from the context which of these identities is represented.

There is an important class of polynomial domains in which a complete enumeration of ideals is known, namely domains of the form $\mathfrak{R}[x]$ where $\mathfrak{R}$ is a (commutative) principal ideal ring. Moreover, a complete characterization of the ideals by numerical (or more general algebraic) invariants is possible if $\mathfrak{R}$ has the further property that each class of associated elements has a uniquely distinguished "normal" representative and each class of residues modulo a given element has a similarly distinguished representative. Such is the case when $\mathfrak{R}=\mathfrak{F}[y]$ where $\mathfrak{F}$ is a field; with each non-zero $f(y)\in\mathfrak{F}[y]$ there is associated a unique $f^*(y)$ with leading coefficient 1 and in each class of residues modulo $f(y)$ there is precisely one $g(y)$ with $\deg g<\deg f$. In the following we shall only be concerned with the case that $\mathfrak{F}$ is the prime field of characteristic p.

A process of enumeration of ideals in $\mathfrak{R}[x]$ was first established by KRONECKER and HENSEL [3] and, independently, by the author [10]; the equivalence of the two systems of enumeration was demonstrated by RÉDEI [6]. The following is an adaptation of the principal result to the case when $\mathfrak{R}[x]=\mathfrak{F}[x,y]$ where $\mathfrak{F}$ is the field of residue classes modulo p.

We first note that every non-zero polynomial of $\mathfrak{F}[y]$,

$$(1.3)\qquad \varphi(y)=a_0+\cdots+a_m y^m,\quad 0\leqq a_i<p\ (i=0,\ldots,m-1),\quad 0<a_m<p$$

can be characterized by a positive integer

$$q=\varphi(p)=a_0+\cdots+a_m p^m;$$

conversely, with each positive integer q there is uniquely associated a polynomial (1.3) of $\mathfrak{F}[y]$. This remark allows us to describe elements of $\mathfrak{F}[y]$ by non-negative integers, and it also introduces a simple ordering of elements of $\mathfrak{F}[y]$ by the rule:

$$(1.31)\qquad \varphi(y)<\psi(y)\quad\text{if and only if}\quad \varphi(p)<\psi(p).$$

To obtain an arbitrary primitive ideal of $\mathfrak{F}[x,y]$ (i. e. an ideal which is not divisible by a non-trivial element of $\mathfrak{F}[x,y]$), we specify

(i) a set of positive integers $d_1,\ldots,d_k$,
(ii) a set of integers $0=s_0<s_1<\cdots<s_k$,
(iii) a set of integers $0\leqq q_{ir}<p^{d_i}$, $\qquad(r=0,\ldots,s_i;\ i=1,\ldots,k)$.

Let $\varphi_{ir}(y)$ be the polynomial (of degree $<d_i$) associated with q_{ir} and define the polynomials $g_0(y)$, $g_i(x,y)$, $(i=1,\ldots,k)$ as follows:

$$(1.41)\qquad g_0(y)=\prod_{i=1}^{k}(y^{d_i}+\varphi_{i,s_i}(y)),$$

$$(1.42)\qquad (y^{d_i}+\varphi_{i,s_i}(y))g_i(x,y)=x^{s_i-s_{i-1}}g_{i-1}(x,y)+\sum_{j=0}^{i-1}\psi_{ij}(x,y)g_j(x,y)$$

where

$$\psi_{ij}(x, y) = \sum_{0 \leqq r < s_{j+1} - s_j} \varphi_{i, s_j + r}(y) x^r \qquad (0 \leqq j < k,\ 1 \leqq i \leqq k). \tag{1.43}$$

Then the ideals

$$\mathfrak{J} = (g_0, g_1, \ldots, g_h) \tag{1.44}$$

which belong to the different systems d_i, s_j, q_{ir} represent exactly once all the primitive ideals of $\mathfrak{P}[x, y]$.[5]

An obvious application of this result is to the structure problem of metabelian p-groups generated by two elements whose commutator subgroup is of the type $(p, \ldots, p)$. For then $h = 1$, $p \equiv 0 (\mathfrak{J})$ in (1.2) and $\mathfrak{J}$ is an ideal in $\mathfrak{P}[u, v]$. The fact that it must also satisfy the second and third condition in (1.2) causes some difficulty which will be resolved in the next section. The actual construction of the groups $\mathfrak{G}$ will be carried out in § 3, and an extension of the result to a further class of metabelian p-groups is discussed in § 4.

2. Since $p = 0$ in $\mathfrak{P}$, the conditions $u^{p^m} \equiv 1, v^{p^m} \equiv 1 (\mathfrak{J})$ are equivalen to $(u-1)^{p^m} \equiv 0, (v-1)^{p^m} \equiv 0 (\mathfrak{J})$. It is convenient to introduce the new variables

$$x = u - 1, \quad y = v - 1$$

corresponding to the operators $\mu = \sigma - 1, \nu = \tau - 1$. Clearly $\mathfrak{A}$ can be regarded as a $\mathfrak{P}[\mu, \nu]$-group and the annulling ideal of A_0 is then an ideal $\mathfrak{J}$ in $\mathfrak{P}[x, y]$ such that

$$x^{p^m} \equiv 0, \quad y^{p^m} \equiv 0 (\mathfrak{J}). \tag{2.0}$$

Since x and y are relatively prime in $\mathfrak{P}[x, y]$, these conditions imply that $\mathfrak{J}$ is a primitive ideal.[6])

The second condition in (2.0) causes no difficulty; it is in fact satisfied if and only if $\varphi_{i, s_i} = 0$ for every i in (1.41). The first condition is much more troublesome; for there seems to be no simple method or algorithm by which to decide from a given system of invariants whether the corresponding $\mathfrak{J}$ contains x^{p^m} or not. Even if such an algorithm existed, it does not seem to be possible to characterize the "good" ideals by means of simple inequalities imposed upon the invariants q_{ir}. Therefore, instead of trying to patch up the system (1.41)—(1.44) to suit conditions (2.0), we shall make a fresh start by assuming right from the beginning that $\mathfrak{J}$ has the property (2.0). Although no explicit use will be made of the Kronecker—Hensel theorem,

---

[5]) [6], p. 200.

[6]) This already follows from the fact that $\mathfrak{P}[x, y]/\mathfrak{J}$ is finite, see RÉDEI [5], § 109.

the work will follow quite closely the method employed for the derivation of (1.41)—(1.44) in [10] and [6].

Suppose that $\mathfrak{I}$ contains the elements x^{p^m}, y^{p^n}. Let l denote the smallest positive integer such that

$$x^l \equiv 0 \ (\mathfrak{I}); \tag{2.01}$$

for $0 \leqq s \leqq l$, denote by c_s the smallest exponent such that

$$y^{c_s} x^s \equiv 0 \ (\mathfrak{I}, x^{s+1}). \tag{2.02}$$

Evidently

$$0 = c_l < c_{l-1} \leqq \cdots \leqq c_0. \tag{2.03}$$

Since (2.0) is assumed, we must have

$$c_0 \leqq p^n, \quad l \leqq p^m. \tag{2.04}$$

In the following we assume that $\mathfrak{I}$ and the corresponding c_s are given.

Lemma 2.1.

$$\varphi(y) x^s \equiv 0 \ (\mathfrak{I}, x^{s+1}), \quad \varphi(y) \in \mathfrak{F}[y] \tag{2.1}$$

implies $\varphi(y) \equiv 0 \ (y^{c_s})$.

We have at any rate $(\varphi(y), y^{c_s}) = y^d$ in $\mathfrak{F}[y]$ where $0 \leqq d \leqq c_s$, hence by (2.02) and (2.1), $y^d x^s \equiv 0 \ (\mathfrak{I}, x^{s+1})$. By the minimal property of c_s, $d \geqq c_s$ hence $d = c_s$, $\varphi(y) \equiv 0 \ (y^{c_s})$.

Lemma 2.2. *If f is an arbitrary polynomial in $\mathfrak{F}[x, y]$ then*

$$f(x, y) \equiv \sum_{s=0}^{l-1} \varphi_s(y) x^s \ (\mathfrak{I}), \quad \varphi_s(y) < y^{c_s} \qquad (s = 0, \ldots, l-1) \tag{2.2}$$

and the coefficients φ_s are uniquely determined by f. The inequality in (2.2) *is in the sense of the ordering* (1.31).

Suppose that we have already proved

$$f \equiv \varphi_0 + \cdots + \varphi_{t-1} x^{t-1} \ (\mathfrak{I}, x^t), \quad \varphi_s < y^{c_s} \quad \text{for} \quad s < t.$$

Write

$$f = \varphi_0 + \cdots + \varphi_{t-1} x^{t-1} + \psi_t x^t \ (\mathfrak{I}, x^{t+1}), \quad \psi_t = \varphi_t + y^{c_t} \varrho_t$$

with $\varphi_t < y^{c_t}$. We have, by (2.02), $\psi_t x^t \equiv \varphi_t x^t \ (\mathfrak{I}, x^{t+1})$ hence $f \equiv \sum_{s=0}^{t} \varphi_s x^s$ $(\mathfrak{I}, x^{t+1})$. The remark that $x^l \equiv 0 \ (\mathfrak{I})$ concludes the proof. Uniqueness follows from Lemma 2.1.

As a corollary we have the result that the elements of $\mathfrak{A}$ can uniquely be written in the form

$$A = A_0^{\sum_{0 \leqq s < l} \varphi_s(\sigma-1)(\tau-1)^s}, \quad \varphi_s(y) < y^{c_s} \qquad (s = 0, \ldots, l-1) \tag{2.21}$$

and the order of $\mathfrak{S}[x, y]/\mathfrak{S}$, hence of $\mathfrak{N}$, is

$$p^h = p^{c_0+\cdots+c_{l-1}}. \tag{2.22}$$

From (2.02) it follows that there exist polynomials $g_s(x, y)$ of the form

$$g_s = y^{c_s}x^s + \sum_{s<t<l} \psi_{st}(y)x^t \equiv 0 \ (\mathfrak{J}) \qquad (s = 0, \ldots, l-1). \tag{2.23}$$

By Lemma 2.1, $\mathfrak{J} = (g_0, \ldots, g_{l-1}, g_l = x^l)$, and we have the problem of enumerating all the essentially different systems (2.23). The chief obstacle in the way of enumeration is that if a system (2.23) is arbitrarily given, it is by no means certain that the c_s which appear in (2.23) are identical with those belonging to $\mathfrak{J} = (g_0, \ldots, g_l)$ in the sense of (2.02). In other words, the c_s in (2.23) do not always possess the required minimum property.

We shall call a system (2.23) *good* if it has the property that

$$\varphi(y)x^s \equiv 0 \quad (g_0, \ldots, g_l, x^{s+1})$$

always implies $\varphi(y) \equiv 0 \ (y^{c_s})$, that is, if Lemma 2.1 is true for $\mathfrak{J} = (g_0, \ldots, g_l)$.

Lemma 2.3. *A system* (2.23) *is good if and only if*

$$xg_s \equiv 0 \ (g_{s+1}, \ldots, g_l) \qquad (s = 0, \ldots, l-1). \tag{2.3}$$

If: Suppose that (2.3) is true for the system $\{g_s\}$. It implies that any expression

$$f_0g_0 + \cdots + f_lg_l, \quad f_s \in \mathfrak{S}[x, y], \qquad (s = 0, \ldots, l)$$

can be written as

$$\sum_{s=0}^{l-1} \varphi_s g_s + f^* g_l, \quad \varphi_s \in \mathfrak{S}[y], \quad f^* \in \mathfrak{S}[x, y].$$

Therefore

$$\varphi(y)x^s \equiv 0 \ (g_s, \ldots, g_l, x^{s+1})$$

for some $s < l$ implies

$$\varphi x^s = \sum_{i=0}^{l-1} \varphi_i g_i + f^* x^{s+1}$$

hence $\varphi_r = 0$ for $r < s$ and $\varphi = \varphi_s y^{c_s}$. By definition, $\{g_s\}$ is a good system.

Only if: We shall prove that if $\{g_s\}$ is good and $x^t f \equiv 0 \ (g_0, \ldots, g_l)$ for some $0 \leqq t \leqq l$ then $x^t f \equiv 0 \ (g_t, \ldots, g_l)$. The statement is trivially true for $t = l$. Suppose it is true for $t+1$ $(t < l)$ and $x^t f \equiv 0 \ (g_0, \ldots, g_l)$. Write $f \equiv \varphi(y) \pmod{x}$ so that $x^t f \equiv x^t \varphi \equiv 0 \ (g_0, \ldots, g_l, x^{t+1})$. This implies, since $\{g_s\}$ is good, that $\varphi = y^{c_t}\psi$, $\psi \in \mathfrak{S}[y]$ and

$$x^t f - \psi g_t + x^{t+1} f^* \equiv 0 \ (g_0, \ldots, g_l)$$

for a suitable $f^* \in \mathfrak{S}[x, y]$. Hence $x^{t+1} f^* \equiv 0 \ (g_0, \ldots, g_l)$ and by the induction hypothesis $x^{t+1} f^* \equiv 0 \ (g_{t+1}, \ldots, g_l)$, $x^t f \equiv 0 \ (g_t, \ldots, g_l)$.

Lemma 2.4. *An ideal $\mathfrak{J}$ which has the property* (2.02) *contains a (necessarily good) set of polynomials* (2.23) *such that*

$$\mathfrak{J} = (g_0, \ldots, g_l \quad - x^l)$$

and

$$xg_s = \sum_{s \leqq t \leqq l} \varphi_{st} g_t, \quad \varphi_{st} \in \mathfrak{S}[y] \tag{2.4}$$

with

$$\varphi_{s,s+1} = y^{c_s - c_{s+1}}, \quad \varphi_{s,t+1} < y^{c_t - c_{t+1}} \quad \text{for} \quad s < t < l. \tag{2.41}$$

Let $s < l$ and suppose that $g_l = x^l$, $g_{l-1}, \ldots, g_{s+1}$ have already been determined so as to satisfy (2.4), (2.41). Let g_s^* be any polynomial $\in \mathfrak{J}$, of degree $< l$ in x and with lowest term $y^{c_s} x^s$. By Lemma 2.3,

$$xg_s^* = \psi_{s+1}(y) g_{s+1} + \cdots + \psi_l(y) g_l$$

hence $\psi_{s+1} = y^{c_s - c_{s+1}} = \varphi_{s,s+1}$. Now suppose that we were able to determine g_s^* so that

$$\psi_{r+1} < y^{c_r - c_{r+1}} \quad \text{for} \quad s < r < t \qquad (t < k).$$

We show the same for $r = t$.

Write $\psi_{r+1} = \varphi_{s,r+1}$ for $r < t$,

$$\psi_{t+1} = \varphi_{s,t+1} + \psi y^{c_t - c_{t+1}}, \quad \varphi_{s,t+1} < y^{c_t - c_{t+1}}.$$

Replace g_s^* by $g_s^{**} = g_s^* - \psi g_t$; then we have

$$xg_s^{**} = xg_s^* - \psi x g_t = \sum_{r=s}^{t-1} \varphi_{s,r+1} g_{r+1} + (\psi_{t+1} - \psi y^{c_t - c_{t+1}}) g_{t+1} +$$

$$+ \sum_{t < r < l} \psi_{r+1}^* g_{r+1} = \sum_{r=s}^{t} \varphi_{s,r+1} g_{r+1} + \sum_{t < r < l} \psi_{r+1}^* g_{r+1}.$$

This proves the Lemma.

To complete the enumeration of the ideals $\mathfrak{J}$ we have to show:

Lemma 2.5. (*a*) *To each system of φ_{st} which satisfy the inequalities* (2.41) *there exists a good system $\{g_s\}$ given by* (2.4), *hence an ideal $\mathfrak{J} = (g_0, \ldots, g_l = x^l)$*; (*b*) *The system φ_{st} is uniquely determined by $\mathfrak{J}$.*

To prove (*a*) it is sufficient to remark that the g_s can obviously be determined recursively from (2.4) and the resulting system is good by Lemma 2.3. In fact the g_s are given explicitly by

$$g_s = \sum_{i=1}^{l-s} \sum_{0 < d_1 < \cdots < d_i = l-s} \varphi_{s,s+d_1} \varphi_{s+d_1,\, s+d_2} \cdots \varphi_{s+d_{i-1},\, i}\, x^{l-i}. \tag{2.51}$$

To prove (b) we have to show that two different systems φ_{st}, φ^*_{st} cannot define the same $\mathfrak{I}$. Suppose that they do belong to the same $\mathfrak{I}$ and suppose also that for some $s<l$, $\varphi_{r,t+1}=\varphi^*_{r,t+1}$ (hence $g_r=g^*_r$) for every $t\geqq r>s$. We have

$$xg_s=\sum_{s<r\leqq l}\varphi_{sr}g_r\,,\quad xg^*_s=\sum_{s<r\leqq l}\varphi^*_{sr}g^*_r=\sum_{s<r\leqq l}\varphi^*_{sr}g_r\,,$$

hence

$$x(g^*_s-g_s)=\sum_{s<r\leqq l}(\varphi^*_{sr}-\varphi_{sr})g_r. \tag{2.52}$$

But $g^*_s\equiv 0\ (g_s,g_{s+1},\ldots,g_k)$ hence $g^*_s=g_s+\sum_{s<r<l}\psi_r g_r$,

$$x(g^*_s-g_s)=\sum_{s<r<l}\psi_r xg_r\,.$$

Suppose that $\psi_r=0$ for $s<r<t$, then

$$x(g^*_s-g_s)=\sum_{t\leqq r<l}\psi_r xg_r=\psi_t\varphi_{t,t+1}g_{t+1}+\sum_{t+1<r\leqq l}\psi^*_r g_r.$$

Comparing with (2.52),

$$\psi_t\varphi_{t,t+1}=\varphi^*_{s,t+1}-\varphi_{s,t+1}<y^{c_t-c_{t+1}}=\varphi_{t,t+1}\,,$$

$$\psi_t=0,\quad (t=s+1,\ldots,l+1),\quad g^*_s=g_s.$$

Lemma 2.5 shows that the g_s given by (2.4), (2.41) form a canonical basis of $\mathfrak{I}$. A more concise form of the basis is obtained if, following RÉDEI, we discard certain unnecessary ones among the g_s. The set $\{c_s\}$ uniquely determines a sequence $0=s_0<s_1<\cdots<s_k=l$ with the property that

$$c_{s_{i+1}}<c_{s_i},\quad c_s=c_{s_i}\quad\text{for}\quad s_i\leqq s<s_{i+1}\qquad (i=0,1,\ldots,k-1).$$

Now from (2.41) we see that $\varphi_{st}=0$ in (2.4) for every t for which $c_{t-1}-c_t=0$ so that

$$xg_s=y^{c_s-c_{s+1}}g_{s+1}+\sum\varphi_{s,s_i}g_{s_i}$$

summed for all i with $s_i>s+1$. Consequently, the g_{s_i} form an ideal basis of $\mathfrak{I}$ and the g_s with $s_i<s<s_{i+1}$ are redundant. If for sake of simplicity we write g_i instead of g_{s_i}, and

$$d_i=c_{s_{i-1}}-c_{s_i}\qquad (i=1,\ldots,k), \tag{2.6}$$

our findings can be summarized as follows:

Definition 2.6. *Given a set of positive integers*

$$d_i>0\qquad (i=1,\ldots,k), \tag{2.61}$$

a set of integers

(2.62) $$0 = s_0 < s_1 < \cdots < s_k = l$$

and a set of integers

(2.63) $$0 \leqq q_{si} < p^{d_i} \qquad (0 < s < s_i,\ 1 \leqq i \leqq k),$$

the ideal

$$\mathfrak{J} = (g_0, \ldots, g_k)$$

of $\mathfrak{F}[x, y]$ *is said to belong to the invariants* (2.61), (2.62), (2.63) *if the* g_i *are obtained from*

(2.64) $$g_k = x^l,$$

(2.65) $$x^{s_{i+1}-s_i} g_i = \sum_{j=i+1}^{k} \psi_{ij}(x, y)\, g_j,$$

(2.66) $$\psi_{ij}(x, y) = \sum_{0 \leqq r < s_{i+1}-s_i} \varphi_{s_{i+1}-r,\,j}(y) x^r \qquad (0 \leqq i < j \leqq k),$$

where

(2.67) $$\varphi_{s_j,\,i} = y^{d_i} \qquad (i = 1, \ldots, k)$$

and $\varphi_{s,i}(y)$ *for* $s < s_i$ *is the polynomial in* $\mathfrak{F}[y]$ *belonging to the integer* q_{si}.

Theorem 1. *To each set of invariants* (2.61), (2.62), (2.63) *there belongs exactly one ideal* $\mathfrak{J}$ *with the property*

(2.71) $$x^l \equiv 0 \ (\mathfrak{J}), \quad y^{c_s} x^s \equiv 0 \ (\mathfrak{J}, x^{s+1}) \qquad (0 \leqq s \leqq l),$$

where

(2.72) $$c_s = \sum_{s_i > s} d_i;$$

c_s *is the smallest integer with property* (2.71).

Conversely, given $\mathfrak{J}$ *with the property* (2.71) *where* c_s *is the smallest such number, and*

(2.73) $$d_i = c_{s_{i-1}} - c_{s_i} \qquad (i = 1, \ldots, k)$$

where

(2.74) $$c_{s_{i+1}} < c_{s_i}, \quad c_s = c_{s_i} \ \text{for} \ s_i \leqq s < s_{i+1} \qquad (i = 0, \ldots, k),$$

there is exactly one system of invariants (2.63) *to which* $\mathfrak{J}$ *belongs.*

It follows from (2.71) that $y^{\sum_{s=0}^{l-1} c_s} \equiv 0 \ (\mathfrak{J})$ so that

(2.75) $$y^{l'} \equiv 0 \ (\mathfrak{J})$$

for some l' with

(2.76) $$l' \leqq \sum_{s=0}^{l-1} c_s.$$

The exact value of l' depends on arithmetic properties of the numbers c_s, q_{st} and cannot be obtained in a straightforward manner. The apparent lack of symmetry in the roles of l and l' is due to the fact that the construction of the canonical basis of Theorem 1 is not symmetrical in x and y.[7]) In fact we can interchange the roles of x and y in the construction of the basis and arrive so at a new set of invariants c_s^*, q_{st}^* which describe exactly the same ideal $\mathfrak{J}$. However, it seems to be rather difficult to formulate an explicit connection between c_s, q_{st} on the one hand, and the „conjugate" invariants c_s^*, q_{st}^* on the other.

3. To construct an arbitrary metabelian group $\mathfrak{G}$ with two generators S, T and commutator subgroup $\mathfrak{A}$ of type $(p, \ldots, p)$, we determine as in § 2 an arbitrary ideal $\mathfrak{J}$ in $\mathfrak{P}[x, y]$ with the property that (2.71) and (2.75) is true for some $l > 0$, $l' > 0$. $\mathfrak{A}$ is defined as a cyclic $P[\sigma, \tau]$-group generated by A_0 and isomorphic to the additive group of the quotient ring $\mathfrak{P}[x, y]/\mathfrak{J}$, through

$$f(x, y) \leftrightarrow A_0^{f(\sigma\ 1, \tau\ 1)}, \quad f(x, y) \in \mathfrak{P}[x, y].$$

Next we specify m, n so that

$$l \leqq p^m, \quad l' \leqq p^n \tag{3.0}$$

where l, l' are the integers in (2.71), (2.75), and define $\mathfrak{G}$ as the group generated by S, T with the relations

$$TS = STA_0 \tag{3.01}$$

$$A_0 S = SA_0^{\sigma} \tag{3.02}$$

$$A_0 T = TA_0^{\tau} \tag{3.03}$$

$$S^{p^m} = H, \quad T^{p^n} = K \tag{3.04}$$

where H, K are suitable elements of $\mathfrak{A}$. Trivially, H and K must be such that

$$H^{\sigma} = H, \quad K^{\tau} = K. \tag{3.05}$$

We also stipulate

$$S^{p^{m-1}} \neq 1, \quad T^{p^{n-1}} \neq 1 \tag{3.06}$$

in case that $H = 1$, $l \leqq p^{m-1}$ or $K = 1$, $l' \leqq p^{n-1}$.

By definition, $\mathfrak{G}$ is an extension of the abelian group $\mathfrak{A}$ of type $(p, \ldots, p)$ by an abelian group $\mathfrak{B}$ of the type (p^m, p^n). A Schreier factorsystem is obtained by taking $S^i T^j$ as the selected representative of $\sigma^i v^j$, $0 \leqq i < p^m$,

---

[7]) This is a defect which is shared by all forms of the canonical basis.

$0 \leqq j < p^n$. The factorsystem

$$C(i_1, j_1; i_2, j_2), \quad 0 \leqq i_\nu < p^m, \quad 0 \leqq j_\nu < p^n, \qquad (\nu = 1, 2)$$

is then defined by

$$S^{i_1} T^{j_1} S^{i_2} T^{j_2} = S^{\{i_1 + i_2\}} T^{\{j_1 + j_2\}} C(i_1, j_1; i_2, j_2), \tag{3.1}$$

$$\{i_1 + i_2\} = i_1 + i_2 - \varepsilon(i_1, i_2) p^m, \quad \{j_1 + j_2\} = j_1 + j_2 - \eta(j_1, j_2) p^n \tag{3.11}$$

where

$$\begin{aligned} \varepsilon(i_1, i_2) &= 0 \quad \text{if} \quad 0 \leqq i_1 + i_2 < p^m \\ &= 1 \quad \text{if} \quad p^m \leqq i_1 + i_2 < 2p^m, \end{aligned} \tag{3.12}$$

$$\begin{aligned} \eta(j_1, j_2) &= 0 \quad \text{if} \quad 0 \leqq j_1 + j_2 < p^n \\ &= 1 \quad \text{if} \quad p^n \leqq j_1 + j_2 < 2p^n. \end{aligned} \tag{3.13}$$

To determine $C(i_1, j_1; i_2, j_2)$ explicitly, we observe first that

$$T^j S^i = S^i T^j A_0^{(1+\sigma+\cdots+\sigma^{i-1})(1+\tau+\cdots+\tau^{j-1})} \qquad (i > 0, \ j > 0). \tag{3.14}$$

(3.14) can be verified by induction with the help of the generating relations (3.01)—(3.03) first for $i = 1$ and $j \geqq 1$ then for fixed $j \geqq 1$ and arbitrary $i \geqq 1$. The formula is also valid for $i = 0$, provided that $1 + \cdots + \sigma^{i-1}$ is interpreted to be 0 for $i = 0$; similarly we agree that $1 + \cdots + \tau^{j-1} = 0$ for $j = 0$.

From (3.14) we obtain immediately

$$S^{i_1} T^{j_1} S^{i_2} T^{j_2} = S^{i_1 + i_2} T^{j_1 + j_2} A_0^{(1+\cdots+\sigma^{i_1-1})(1+\cdots+\tau^{j_1-1})\tau^{j_2}}$$

and hence by an easy computation from (3.05), (3.1), (3.11)

$$C(i_1, j_1; i_2, j_2) = A_0^{(1+\cdots+\sigma^{i_2-1})(1+\cdots+\tau^{j_1-1})\tau^{j_2}} H^{\varepsilon(i_1, i_2)\tau^{j_1+j_2}} K^{\eta(i_1, j_2)}. \tag{3.15}$$

The Schreier conditions to be satisfied are

$$\begin{aligned} &C(i_1, j_1; \{i_2 + i_3\}, \{j_2 + j_3\}) C(i_2, j_2; i_3, j_3) = \\ &= C(\{i_1 + i_2\}, \{j_1 + j_2\}; i_3, j_3) C(i_1, j_1; i_2, j_2)^{\sigma^{i_3}\tau^{j_3}}. \end{aligned} \tag{3.16}$$

If we put here first $i_1 = 0, i_2 = 1, i_3 = p^m - 1, j_1 = 1, \ j_2 = j_3 = 0$ then $i_1 = i_2 = 0, i_3 = 1, \ j_1 = p^n - 1, j_2 = 1, j_3 = 0$, we obtain

$$H^{1-\tau} = A_0^{1+\cdots+\sigma^{p^m-1}}, \quad K^{\sigma-1} = A_0^{1+\cdots+\tau^{p^n-1}},$$

hence with (3.05)

$$H^{\sigma-1} = 1, \quad H^{\tau-1} = A_0^{-(1+\cdots+\sigma^{p^m-1})}, \tag{3.17}$$

$$K^{\sigma-1} = A_0^{1+\cdots+\tau^{p^n-1}}, \quad K^{\tau-1} = 1. \tag{3.18}$$

Conversely one can verify that (3.17), (3.18) are sufficient for all Schreier conditions (3.16) to be satisfied so that (3.17), (3.18) are the only restrictions to which H and K are subjected.

Let us write

$$H = A_0^{h(\sigma-1,\tau-1)}, \quad K = A_0^{h(\sigma-1,\tau-1)}; \tag{3.19}$$

we then have the condition that

$$xh(x,y) \equiv 0, \quad yh(x,y) \equiv -x^{p^m-1} \ (\mathfrak{J}) \tag{3.21}$$

$$xk(x,y) \equiv y^{p^n-1}, \quad yk(x,y) \equiv 0 \ (\mathfrak{J}). \tag{3.22}$$

We want to characterize all polynomials $h(x,y)$, $k(x,y)$ which satisfy these congruences.

Suppose first that

$$l < p^m \tag{3.23}$$

so that $x^{p^m-1} \equiv 0 \ (\mathfrak{J})$ and

$$xh(x,y) \equiv yh(x,y) \equiv 0 \ (\mathfrak{J}) \tag{3.24}$$

is valid instead of (3.21).

Now, a polynomial $h(x,y)$ which satisfies $xh \equiv 0 \ (\mathfrak{J})$ can be written uniquely in the form

$$h \equiv \sum_{s=1}^{l} \varphi_s(y) \frac{1}{x} g_s^* \ (\mathfrak{J}) \qquad (0 \leqq \varphi_s < y^{e_{s-1}-e_s}) \tag{3.25}$$

where the g_s^* are the polynomials g_s of Lemma 2.4. This can be shown by the same argument as used in the proof of Lemmas 2.4 and 2.5. Since $\varphi_s(y) = 0$ if $c_{s-1} - c_s = 0$, we can also write

$$h \equiv \sum_{j=1}^{k} \psi_i(y) \frac{1}{x} g_i \ (\mathfrak{J}) \qquad (0 \leqq \psi_i (= \varphi_{s_i}) < y^{d_i}) \tag{3.26}$$

where $g_i = g_{s_i}^*$. The second condition in (3.24) can now be expressed as

$$\sum_{j=1}^{k} y\psi_j(y) \frac{1}{x} g_j \equiv 0 \ (\mathfrak{J}). \tag{3.27}$$

Lemma 3.3. *Let $\varphi_{sj}(y)$ be as in Theorem* 1,

$$a_{ij} = \varphi_{s_i,j}(0) \qquad (1 \leqq i \leqq j \leqq k). \tag{3.3}$$

Let $(\xi_1, \ldots, \xi_k)$ be a solution vector over $\mathfrak{F}$ of the linear homogeneous system

$$\sum_{i=1}^{j} \xi_i a_{ij} = 0 \qquad (j = 1, \ldots, k), \tag{3.31}$$

and set

$$y\psi_j(y) = -\sum_{i=1}^{j} \xi_i \varphi_{s_i,j}(y) \qquad (j = 1, \ldots, k); \tag{3.32}$$

then the congruence (3.27) *holds.*

Conversely, every set of $\psi_j \in \mathfrak{S}[y]$, $(j = 1, \ldots, k)$ *for which* (3.27) *is true can be written uniquely in the form* (3.32) *where* $(\xi_1, \ldots, \xi_k)$ *is a solution vector of* (3.31).

It follows from Lemma 3.3 that an $h(x, y)$ which satisfies (3.24) can be characterized completely by a solution vector $\xi = (\xi_1, \ldots, \xi_k)$ of (3.31). Note that the $\psi_j(y)$ defined by (3.32) are polynomials, because of (3.31). Note also that

$$a_{ii} = 0 \qquad (i = 1, \ldots, k) \tag{3.33}$$

from (3.36) below, so that the rank of the system (3.31) is always less than k. In particular, $\xi_i = 0$ for $1 \leqq i < k$, $\xi_k \neq 0$ is a non-zero solution of (3.31). The corresponding $h(x, y)$ is given by

$$h(x, y) = \xi_k y^{d_k - 1} x^{s_k - 1}. \tag{3.34}$$

The proof of the Lemma is based on the formula

$$\sum_{j=i}^{k} \varphi_{s_i,j}(y) \frac{1}{x} g_j \equiv 0 \ (\mathfrak{J}) \qquad (i = 1, \ldots, k) \tag{3.35}$$

with

$$\varphi_{s_i,i} = y^{d_i}, \quad 0 \leqq \varphi_{s_i,j}(y) < y^{d_j} \qquad (i < j \leqq k). \tag{3.36}$$

The formula follows directly from (2.65), (2.66) and the fact that $g_i \equiv 0$ $(\mathfrak{J})$.

Suppose now that the ξ_i are a solution of (3.31) and ψ_j is given by (3.32). Substitution into the left hand member of (3.27) gives

$$\sum_{j=1}^{k} y\psi_j \frac{1}{x} g_j = \sum_{j=1}^{k} \sum_{i=1}^{j} \xi_i \varphi_{s_i,j} \frac{1}{x} g_j = \sum_{i=1}^{k} \xi_i \sum_{j=i}^{k} \varphi_{s_i,j} \frac{1}{x} g_j \equiv 0 \ (\mathfrak{J})$$

by (3.35), as required.

Conversely, suppose that the ψ_j satisfy (3.27); then

$$\sum_{j=1}^{q} y\psi_j \frac{1}{x} g_j \equiv 0 \ (\mathfrak{J}, x^{s_q}), \qquad (q = 1, \ldots, k) \tag{3.37}$$

and we show that (3.37) holds for $q \leqq r$ $(r \leqq k$ given) only if $\psi_1, \ldots, \psi_r$ are of the form (3.32) where ξ_j $(j = 1, , \ldots, r)$ is a solution of (3.31) for $j = 1, \ldots, r$.

Suppose that the statement is true for $r-1$ (in the case of $r=1$ the assumption is empty), i. e. ψ_j for $j<r$ is of the form (3.32). Substitution into the left hand member of (3.37) gives, by (3.35) and the definition of g_j,

$$y\psi_r \frac{1}{x} g_r + \sum_{j=1}^{r-1} y\psi_j \frac{1}{x} g_j = y\psi_r \frac{1}{x} g_r + \sum_{j=1}^{r-1} \sum_{i=1}^{j} \xi_i \varphi_{s_i,j} \frac{1}{x} g_j =$$

$$= y\psi_r \frac{1}{x} g_r + \sum_{i=1}^{r-1} \xi_i \sum_{j=i}^{r-1} \varphi_{s_i,j} \frac{1}{x} g_j$$

$$\equiv y\psi_r \frac{1}{x} g_r - \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} \frac{1}{x} g_r \quad (\mathfrak{J}, x^{s_r})$$

$$\equiv \left(y\psi_r - \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} \right) y^{c_{s_r}} x^{s_r-1} \quad (\mathfrak{J}, x^{s_r}),$$

hence by (3.37),

$$\left(y\psi_r - \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} \right) y^{c_{s_r}} x^{s_r-1} \equiv 0 \quad (\mathfrak{J}, x^{s_r}).$$

This can only hold, by definition of the s_r and c_s, if

$$\left(y\psi_r - \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} \right) y^{c_{s_r}} \equiv 0 \quad (y^{c_{s_r-1}}),$$

$$y\psi_r - \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} \equiv 0 \quad (y^{d_r}),$$

i. e. if

$$y\psi_r = \sum_{i=1}^{r-1} \xi_i \varphi_{s_i,r} + \xi_r y^{d_r}$$

for some $\xi_r \in \mathfrak{S}$ which is uniquely determined by ψ_r (since $\varphi_{s_i,r} < y^{d_r}$, $(i=1,\ldots,r-1)$, and $\psi_r < y^{d_r}$). Hence

$$y\psi_r = \sum_{i=1}^{r} \xi_i \varphi_{s_i,r}$$

and the right hand side must be divisible by y, implying

$$\sum_{i=1}^{r} \xi_i a_{ir} = 0.$$

This proves the statement and the Lemma.

If $l=p^m$ then we have (3.21) instead of (3.24) and

$$\sum_{i=1}^{k} y\psi_i \frac{1}{x} g_i + x^{l-1} \equiv 0 \quad (\mathfrak{J}) \tag{3.38}$$

instead of (3.27). A trivial modification of the proof of Lemma 3.3 shows that the solutions of (3.38) are given by

$$y\psi_j(y) = \sum_{i=1}^{j} \xi_i \varphi_{s_i,j}(y) - \delta_{jk} \qquad (j = 1, \ldots, k) \tag{3.39}$$

where $(\xi_1, \ldots, \xi_k)$ is a solution of

$$\sum_{i=1}^{j} \xi_i a_{ij} = \delta_{jk} \qquad (j = 1, \ldots, k) \tag{3.40}$$

($\delta_{jk} = 1$ for $j = k$, 0 for $j \neq k$). Hence not all systems of invariants are admissible but only those for which (3.40) has a solution vector, that is, for which the vector $(a_{1k}, \ldots, a_{kk})$ is linearly independent of the $(a_{1j}, \ldots, a_{jj}, 0, \ldots, 0)$ $(j = 1, \ldots, k-1)$.

To characterize $k(x, y)$ in (3.22) we can use the same method as for $h(x, y)$, provided that $l' < p^n$. The equations to be satisfied are then $xk(x, y) \equiv \equiv yk(x, y) \equiv 0$ $(\mathfrak{S})$ and the $k(x, y)$ are obtained from Lemma 3.3. If $l' = p^n$, however, the method cannot be used directly and it seems best to make use of the conjugate invariants c_s^*, s_i^*, q_{si}^*, obtained by interchanging the roles of x and y in Theorem 1. If $\varphi_{si}^*(y)$ are the corresponding polynomials and $a_{ij}^* = \varphi_{s_i^*,j}^*(0)$ then $k(x, y)$ is given by

$$k(x, y) = \sum_{j=1}^{k^*} \psi_j^*(y) \frac{1}{x} g_j^*, \tag{3.26*}$$

$$y\psi_j^*(y) = \sum_{i=1}^{j} \xi_i^* \varphi_{s_i^*,j}^*(y) + \delta_{jk^*} \qquad (j = 1, \ldots, k^*) \tag{3.39*}$$

where $\xi^* = (\xi_1^*, \ldots, \xi_{k^*}^*)$ is a solution vector of

$$\sum_{i=1}^{j} \xi_i^* a_{ij}^* = -\delta_{jk^*} \qquad (j = 1, \ldots, k^*). \tag{3.40*}$$

For the sake of uniformity it is perhaps better to use the conjugate invariants even if $l' < p^n$; we then have

$$y\psi_j^*(y) = \sum_{i=1}^{j} \xi_i^* \varphi_{s_i^*,j}^*(y) \qquad (j = 1, \ldots, k^*), \tag{3.32*}$$

$$\sum_{i=1}^{j} \xi_i^* a_{ij}^* = 0 \tag{3.31*}$$

with $k(x, y)$ given by (3.26*).

Theorem 2. *A metabelian p-group with two generators S, T and commutator subgroup of type* $(p, \ldots, p)$ *is completely specified by* (i) *a set of integers* d_i, s_i, q_{si} *subject to the conditions* (2.61), (2.62) *and* (2.63) *with*

$l > 1$, (ii) *integers* m, n *subject to* (3.0), (iii) *solution vectors* ξ, ξ^s *of* (3.31), (3.31^s) *if there is strict inequality in* (3.0) *or of* (3.40), (3.40*) *if the equality sign is valid in* (3.0).

The construction of the group $\mathfrak{G}$ *is carried out in the following steps:*

1. *Construct a cyclic* $\mathfrak{F}[\sigma-1, \tau-1]$*-group* $\mathfrak{A} = \{A_0\}$ *with annulling ideal* $\mathfrak{I}$ *where* $\mathfrak{I}$ *is the ideal belonging to the invariants* (i) *according to Definition* 2.6.

2. *Define* $H \in \mathfrak{A}$, $K \in \mathfrak{A}$ *as in* (3.19), *with* $h(x, y), k(x, y)$ *given by* (3.26), (3.26*) *where* ξ, ξ^s *are the invariants* (iii).

3. *Define* $\mathfrak{G}$ *by the generating relations* (3.01)—(3.04) *where* m, n *are the invariants* (ii).

We have called the system of numbers (i), (ii), (iii) of Theorem 2 invariants of $\mathfrak{G}$; in fact, to each such system there belongs precisely one metabelian $\mathfrak{G}$ and each $\mathfrak{G}$ with the specified properties can be obtained in this manner. Nevertheless the system (i), (ii), (iii) is not a true system of invariants; for $\mathfrak{G}$ can usually be obtained from several different such systems. There are two ways in which one can change the invariants of a given $\mathfrak{G}$.

First, one can select new representatives

$$S_1 = SB, \quad T_1 = TC, \qquad B \in \mathfrak{A}, \quad C \in \mathfrak{A} \tag{3.41}$$

of the cosets σ, τ of $\mathfrak{B} = \mathfrak{G}/\mathfrak{A}$. Secondly one can replace σ, τ by new basis elements of $\mathfrak{B}$.

The first of these changes implies a replacement of $A_0 = T^{-1}S^{-1}TS$ by

$$A_1 = T_1^{-1}S_1^{-1}T_1S_1 = T^{-1}S^{-1}TSB^{1-\tau}C^{\sigma-1} = A_0B^{-(\tau-1)}C^{\sigma-1}$$

and a replacement of $H = S^{p^m}$, $K = T^{p^n}$ by

$$H_1 = S_1^{p^m} = S^{p^m}B^{1+\sigma+\cdots+\sigma^{p^m-1}} = HB^{(\sigma-1)p^m-1}, \quad K_1 = T_1^{p^n} = KC^{(\tau-1)p^{n-1}}.$$

These changes do not affect the ideal $\mathfrak{I}$, hence s_i, d_i, q_{si}, in any way, also not m and n. Furthermore

$$A^{h(\sigma-1,\tau-1)} = A^{h(\sigma-1,\tau-1)}B^{-(\tau-1)h(\sigma-1,\tau-1)}C^{(\sigma-1)h(\sigma-1,\tau-1)} = HB^{(\sigma-1)p^m-1} = H_1$$

by (3.17) and (3.19), and similarly

$$A_1^{k(\sigma-1,\tau-1)} = K_1.$$

Hence, $h(x, y), k(x, y)$ remain unchanged and the system of invariants of $\mathfrak{G}$ is completely independent of the particular representatives (3.41) of the cosets σ, τ.

Not quite so simple is the case with the second type of change, viz. transition to a new basis in $\mathfrak{B}$. Even the simplest of these transformations, namely interchange of the two basis elements, is non-trivial as it causes the invariants to be replaced by their conjugate system. Other transformations of the basis elements may change the ideal $\mathfrak{I}$ itself. The enumeration of the groups $\mathfrak{G}$ in Theorem 2. cannot be regarded as wholly satisfactory until the problem of selection of a well-defined representative among equivalent systems of invariants is solved.[8])

4. There is a further class of metabelian p-groups with two generators which can be determined by the previous method, namely the ones which contain an abelian normal subgroup $\mathfrak{A}$ such that $\mathfrak{B} = \mathfrak{G}/\mathfrak{A}$ is cyclic. We shall indicate briefly the necessary steps. It can be assumed that $\mathfrak{A}$ is a smallest subgroup with the above property. Let S, T be generators of $\mathfrak{G}$. At least one of them, say T, is a representative of a generating coset $\tau = T\mathfrak{A}$ of $\mathfrak{B}$. Then $S = T^q A_0$, $A_0 \in \mathfrak{A}$, hence T and A_0 generate S, therefore they generate $\mathfrak{G}$.

Take a fixed $A_0 \in \mathfrak{A}$ such that T and A_0 generate $\mathfrak{G}$. $\mathfrak{A}$ is now a $\mathcal{C}[\tau]$-group and as such it is generated by A_0. For, if $\mathfrak{A}^*$ is the subgroup of elements $A_0^{f(\tau)}$ then clearly $\mathfrak{A}^* \subseteq \mathfrak{A}$ and $\mathfrak{G}/\mathfrak{A}^*$ is cyclic, hence by the assumption on $\mathfrak{A}$, $\mathfrak{A}^* = \mathfrak{A}$.

The annulling ideal of A_0 is an ideal $\mathfrak{j}$ in $\mathcal{C}[x]$ under the correspondence $\tau - 1 \leftrightarrow x$ with the properties

$$p^h \equiv 0 \ (\mathfrak{j}) \tag{4.11}$$

$$x^l \equiv 0 \ (\mathfrak{j}) \tag{4.12}$$

for suitable positive integers h, l. The first is trivial (p^h is simply the exponent of $\mathfrak{A}$), the second follows from

$$\tau^{p^n} = 1 \tag{4.13}$$

where p^n is the order of $\mathfrak{B}$. For by (4.13), $(\tau-1)^{p^n} \equiv 0 \ (p)$, $(\tau-1)^{hp^n} \equiv 0 \ (p^h)$ hence by (4.11), $(\tau-1)^{hp^n} \equiv 0 \ (\mathfrak{j})$.

If it were not for the condition (4.12), the enumeration of the ideals $\mathfrak{j}$ would be a matter of straightforward application of the Kronecker—Hensel theorem. Because of (4.12) we must proceed as in § 2.

Definition 4.2. *Given a set of positive integers*

$$d_i > 0 \qquad (i = 1, \ldots, k), \tag{4.21}$$

a set of integers

$$0 = s_0 < s_1 < \cdots < s_k = l \tag{4.22}$$

[8]) The problem is analogous to (though not identical with) the determination of all non-isomorphic cyclic rings, as discussed by Rédei in [5], § 109.

and a set of integers

$$0 \leqq q_{si} < p^{d_i} \qquad (0 < s < s_i, \quad 1 \leqq i \leqq k) \tag{4.23}$$

the ideal

$$\mathfrak{J} = (g_0, \ldots, g_k)$$

is said to belong to the invariants (4.21), (4.22), (4.23)[9]) *if the* g_i *are obtained from*

$$g_k = x^l \tag{4.24}$$

$$x^{s_{i+1}-s_i} g_i = \sum_{j=i+1}^{k} \psi_{ij}(x) g_j \tag{4.25}$$

where

$$\psi_{ij}(x) = \sum_{0 \leqq r < s_{i+1}-s_i} q_{s_{i+1}-r} x^r \qquad (0 \leqq i < j \leqq k) \tag{4.26}$$

with

$$q_{s_i, i} = p^{d_i} \qquad (i = 1, \ldots, k). \tag{4.27}$$

By trivial modifications of the argument in § 2 one obtains

Theorem 3. *To each set of invariants* (4.21), (4.22), (4.23) *there belongs exactly one ideal* $\mathfrak{J}$ *with the property*

$$x^l \equiv 0 \ (\mathfrak{J}), \quad p^{e_s} x^s \equiv 0 \ (\mathfrak{J}, x^{s+1}) \qquad (0 \leqq s < l) \tag{4.31}$$

where

$$c_s = \sum_{s_i > s} d_i. \tag{4.32}$$

c_s *is the smallest number with property* (4.31).

Conversely, given $\mathfrak{J}$ *with the property* (4.31) *where* c_s *is the smallest such number, and*

$$d_i = c_{s_{i-1}} - c_{s_i} \qquad (i = 1, \ldots, k) \tag{4.33}$$

where

$$c_{s_i+1} < c_{s_i}, \quad c_s = c_{s_i} \ \text{for} \ s_i \leqq s < s_{i+1} \qquad (i = 0, \ldots, k), \tag{4.34}$$

there is exactly one system of invariants (4.23) *to which* $\mathfrak{J}$ *belongs.*

From (4.31) we conclude that there is a smallest h and m such that

$$p^h \equiv 0 \ (\mathfrak{J}), \quad (x+1)^{p^m} \equiv 1 \ (\mathfrak{J}). \tag{4.35}$$

The exact values of h and m depend on arithmetic properties of c_s, q_{si} and

[9]) $\mathfrak{J}$ is an ideal in $\mathfrak{C}[x]$ so that there is no danger of confusion with Definition 2.6.

must be determined in each individual case; the estimates

$$h \leqq \sum_{s=0}^{l-1} c_s, \quad p^m < l p^h \tag{4.36}$$

are trivial. The order of $\mathcal{C}[x]/\mathfrak{J}$ is p^r, $r = \sum_{s=0}^{l-1} c_s$.

To construct an arbitrary metabelian group $\mathfrak{S}$ with the required properties we start from an ideal $\mathfrak{J}$ with $l > 1$, as obtained in Theorem 3, and define a cyclic $\mathcal{C}[\tau]$-group $\mathfrak{A}$ generated by A_0 and isomorphic to the additive group of the quotient ring $\mathcal{C}[x]/\mathfrak{J}$ through

$$f(x) \longleftrightarrow A_0^{f(\tau-1)}, \quad f(x) \in \mathcal{C}[x].$$

We then determine n so that

$$n \geqq m \tag{4.4}$$

where m is the integer in (4.35), and define $\mathfrak{S}$ by the relations

$$A_0 T = T A_0^{\tau} \tag{4.41}$$

$$T^{p^n} = K = A_0^{k(\mu)} \quad \mu = \tau - 1, \tag{4.42}$$

where $k(x)$ is a suitable polynomial of $\mathcal{C}[x]$. By taking T^j $(0 \leqq j < p^n)$ as the selected representative of τ^j, the Schreier conditions are satisfied if

$$K^{\tau} = K \tag{4.43}$$

i. e. if

$$x k(x) \equiv 0 \ (\mathfrak{J}). \tag{4.44}$$

A polynomial which satisfies (4.44) can be written uniquely in the form

$$k(x) = \sum_{i=1}^{k} b_i \frac{1}{x} g_i(x), \quad 0 \leqq b_i < p^{d_i} \qquad (i = 1, \ldots, k) \tag{4.45}$$

where the $d_i, g_i(x)$ are from Theorem 3. As there are no further conditions on $k(x)$, K is completely characterized by a set of numbers b_i $(i = 1, \ldots, k)$ to be chosen freely in the range $0 \leqq b_i < p^{d_i}$.

A simple calculation shows that for a fixed set of c_s, the number of ways in which one can assign values to the invariants q_{s_i} and b_i is p^r, $r = \sum_{s=0}^{l-1} c_s$, which is just the order of $\mathfrak{A}$. Hence the total number of distinct $\mathcal{C}[\tau]$-groups of order p^r, to which an element K with the property (4.43) has been assigned, is

$$p^r N(r), \tag{4.46}$$

where $N(r)$ is the number of unrestricted partitions of r. For comparison note that $N(r)$ is the number of distinct (ordinary) abelian groups of order p^r.

Turning now to the question of equivalence of the various systems of invariants b_i, d_i, q_{si}, the following changes must be considered:

(a) Replace T by a new representative $T_1 = TB$, $B \in \mathfrak{A}$ of the coset τ.

(b) Replace A_0 by a new generator $A_1 = A_0^{\varphi(t)}$ of $\mathfrak{A}$.

(c) Replace τ by a new generator $\tau_1 = \tau^j$, $(j, p) = 1$ of $\mathfrak{B}$.

(d) Replace $\mathfrak{A}$ by another minimal abelian normal subgroup $\mathfrak{A}^*$ with cyclic quotient group $\mathfrak{B}^* = \mathfrak{G}/\mathfrak{A}^*$.

(a) and (b) affect the numbers b_i, but not the other invariants. They cause $k(x)$ to be replaced by

$$ak(x) + b\pi_n(x) \tag{4.51}$$

modulo $\mathfrak{J}$ where

$$\pi_n(x) = \sum_{i=1}^{p^n} \binom{p^n}{i} x^{i-1} \tag{4.52}$$

and a, b are integers. Note that $x\pi_n(x) = x^{p^n} - 1 \equiv 0$ $(\mathfrak{J})$, so that (4.51) is a legitimate transformation.

A replacement of τ by $\tau_1 = \tau^j$, $(j, p) = 1$ induces a transformation of $\mathfrak{J}$ into the ideal $\mathfrak{J}^*$ formed by all polynomials which have the form $f^*(x) = f((x+1)^i - 1)$ where $f(x) \in \mathfrak{J}$ and $ij \equiv 1 \pmod{p^n}$. Neither of the transformations (a), (b), (c) can be expressed in the form of a simple explicit transformation law of the b_i, q_{si}.

The existence of a second subgroup $\mathfrak{A}^*$ as envisaged under (d) is rather exceptional. It requires T to commute with each element of the commutator subgroup K, which is so if and only if

$$x^2 \equiv 0 \ (\mathfrak{J}), \tag{4.53}$$

i. e. $l = 2$ in (4.22). $\mathfrak{A}^*$ is then the subgroup generated by T and K.

There are two classes of invariants compatible with $l = 2$:

$$k = 1, \quad s_0 = 0, \quad s_1 = 2 \tag{4.54}$$

$$k = 2, \quad s_0 = 0, \quad s_1 = 1, \quad s_2 = 2. \tag{4.55}$$

In the first case we have (with $d = d_1$, $q = q_{11}$, $b = b_1$)

$$g_0(x) = p^d + qx, \quad g_1(x) = x^2, \quad k(x) = bx,$$
$$0 \leqq q < p^d, \quad 0 \leqq b < p^d, \quad n \geqq m = d.$$

It is easy to verify that this system is equivalent to

$$g_0(x) = p^d + p^{a_1}x, \quad g_1(x) = x^2 \tag{4.56}$$

$$k(x) = p^{a_2}x, \quad 0 \leqq a_\nu \leqq d \qquad (\nu = 1, 2) \tag{4.57}$$

where in the case of $a_\nu = d$ we can replace p^{a_ν} by 0. The order of $\mathfrak{A}/\mathfrak{K}$ is p^d, the order of $\mathfrak{A}^*/\mathfrak{K}$ is $p^n \geqq p^d$ so that the minimum condition on $\mathfrak{A}$ is satisfied.

In the case of $n = d$, $\mathfrak{A}$ and $\mathfrak{A}^*$ have equal orders and therefore they are both minimal. We can make an appropriate selection e. g. by requiring that A_0 should have a largest possible order. This leads to the supplementary conditions

$$n < d \quad \text{or} \quad n = d, \quad a_2 \geqq a_1 \tag{4.59}$$

which specify the canonical system (4.56), (4.57) uniquely.

Finally we consider invariants of the type (4.55). The corresponding canonical basis has the form

$$g_0(x) = p^{a_1+d_2} + qx, \quad 0 \leqq q < p^{d_2} \tag{4.60}$$
$$g_1(x) = p^{a_2}x, \quad g_2(x) = x^2$$

with

$$k(x) = b_1 p^{d_2} + b_2 x, \quad 0 \leqq b_\nu < p^{d_\nu} \qquad (\nu = 1, 2). \tag{4.61}$$

It can be shown that this system is equivalent to one with

$$q = p^{a_2}, \quad 0 \leqq a_2 \leqq d_2 \tag{4.62}$$
$$b_1 = p^{a_1}, \quad 0 \leqq a_1 \leqq d_1, \quad 0 \leqq b_2 < p^{a_2}.$$

The minimum condition on $\mathfrak{A}$ demands that $n + d_1 - a_1 \geqq d_1 + d_2$, i. e.

$$n \geqq a_1 + d_2 = a_1 + m. \tag{4.63}$$

If $n = a_1 + d_2$ then also $\mathfrak{A}^*$ is minimal and the invariants related to $\mathfrak{A}^*$ have the same form (4.60)—(4.62) as those related to $\mathfrak{A}$, with possibly different values of a_2, b_2. We can use either of the two systems to characterize this particular type of $\mathfrak{G}$.

5. In conclusion we set up a list of all "known" types of finite metabelian p-groups, that is classes of groups whose members have been determined explicitly. The catalogue does not contain every individual metabelian p-group which has ever been determined or described; a notable example of an exception is the maximal metabelian p-group with k generators and exponent p, determined by MEIER-WUNDERLI [4], which does not belong to either of these classes. But it should nevertheless give a fair idea of the extent to which the general structure problem of metabelian p-groups has been settled.

In the list below, $\mathfrak{A}$ denotes an abelian normal subgroup of the metabelian p-group $\mathfrak{G}$ with stated properties.

(1) $\mathfrak{G}$ of exponent p and generated by at most 5 elements.[10])
(2) $\mathfrak{G}/\mathfrak{N}$ of order p.[11])
(3) $\mathfrak{N}$ of exponent p, $\mathfrak{G}/\mathfrak{N}$ cyclic.[12])
(4) $\mathfrak{G}/\mathfrak{N}$ cyclic, $\mathfrak{G}$ generated by two elements.[13])
(5) $\mathfrak{N}$ of exponent p, $\mathfrak{G}/\mathfrak{N}$ abelian, $\mathfrak{G}$ generated by two elements.[13])

Numerous other metabelian group determinations of the past were omitted because they were included in at least one of the above classes. For example the classical Hölder case when both $\mathfrak{N}$ and $\mathfrak{G}/\mathfrak{N}$ are cyclic is included in (4).

Bibliography

. R. Brahana, Finite metabelian groups, *American Journal of Math.*, **62** (1940), 365—379.
[2] ——— Finite metabelian groups, *American Journal of Math.*, **73** (1951), 539—555.
[3] L. Kronecker and K. Hensel, *Vorlesungen über Zahlentheorie* (Leipzig, 1901).
[4] H. Meier-Wunderli, Metablesche Gruppen, *Commentarii Math. Helvetici*, **25** (1951), 1—10.
[5] L. Rédei, *Algebra I* (Budapest, 1954).
[6] ——— Äquivalenz der Sätze von Kronecker—Hensel und von Szekeres, *Acta Sci. Math.*, **17** (1956), 198—202.
[7] L. L. Scott, Finite metabelian groups, *Duke Math. Journal*, **20** (1953), 405—414.
[8] G. Szekeres, On a certain class of finite metabelian groups, *Annals of Math.*, **49** (1948), 43—52.
[9] ——— Determination of finite metabelian groups, *Transactions American Math. Society*, **66** (1949), 1—43.
[10] ——— A canonical basis for ideals, *American Math. Monthly*, **59** (1952), 379—386.

(Received March 17, 1960)

[10]) Brahana [1] and [2], also an extension to 6 generators by Scott [7], but the enumeration is not complete.
[11]) Determined in [9].
[12]) Determined in [8].
[13]) Determined in the present paper.

Über die orthogonalen Funktionen. IX
(Absolute Summation)

Von KÁROLY TANDORI in Szeged

Herrn Professor László Rédei zum 60. Geburtstag

Das n-te $(C, 1)$-Mittel der Orthogonalreihe

$$\sum_{k=0}^{\infty} a_k \varphi_k(x) \tag{1}$$

sei mit $\sigma_n(x)$ bezeichnet. Wir sagen, daß (1) an der Stelle x $|C, 1|$-summierbar ist, wenn

$$\sum_{n=0}^{\infty} |\sigma_{n+1}(x) - \sigma_n(x)| < \infty \tag{2}$$

gilt. Wir setzen zur Abkürzung

$$A_m = (a_{2^m+1}^2 + \cdots + a_{2^{m+1}}^2)^{1/2} \qquad (m = 0, 1, \ldots).$$

Es wird der folgende Satz bewiesen:

Satz. *Die Bedingung*

$$\sum_{m=0}^{\infty} A_m < \infty \tag{3}$$

ist notwendig und hinreichend dafür, daß die Orthogonalreihe (1) *für jedes orthonormierte Funktionensystem* $\{\varphi_k(x)\}$ *im Grundintervall* $[a, b]$ *fast überall* $|C, 1|$*-summierbar ist.*

Früher hat G. ALEXITS[1]) bewiesen, daß im Falle $a_k = O(q_k)$, wo $\{q_k\}$ eine positive, monoton nichtwachsende Zahlenfolge mit der Eigenschaft

$$\sum_{k=1}^{\infty} q_k k^{-\frac{1}{2}} < \infty$$

[1]) G. ALEXITS, Ein Summationssatz für Orthogonalreihen, *Acta Math. Acad. Sci. Hung.*, 7 (1956), 5—9.

bedeutet, die Orthogonalreihe (1) für jedes orthonormierte Funktionensystem $\{\varphi_k(x)\}$ in $[a, b]$ fast überall $(C, 1)$-summierbar ist.

In einem Brief hat mich Herr G. ALEXITS darauf aufmerksam gemacht, daß aus den Bedingungen seines Satzes auch (2) in $[a, b]$ fast überall folgt. Da für eine positive, monoton nichtwachsende Folge $\{a_k\}$ die Beziehungen (3) und

$$\sum_{k=1}^{\infty} a_k k^{-\frac{1}{2}} < \infty$$

gleichwertig sind, ist unser Satz offensichtlich eine Verallgemeinerung des Satzes von G. ALEXITS.

Beweis des Satzes. *Hinlänglichkeit.* Ohne Beschränkung der Allgemeinheit kann $a_0 = a_1 = 0$ angenommen werden. Auf Grund von (3) ist

$$\sum_{n=1}^{\infty} \int_a^b |\sigma_{n+1}(x) - \sigma_n(x)|\, dx = O(1) \sum_{n=1}^{\infty} \left\{ \int_a^b (\sigma_{n+1}(x) - \sigma_n(x))^2 dx \right\}^{1/2} =$$

$$= O(1) \sum_{n=1}^{\infty} \frac{1}{n^2} \left\{ \sum_{k=2}^{n+1} k^2 a_k^2 \right\}^{1/2} = O(1) \sum_{n=1}^{\infty} \frac{1}{n^2} \sum_{m=0}^{[\log(n+1)]} 2^{m+1} A_m =$$

$$= O(1) \sum_{m=0}^{\infty} A_m 2^{m+1} \sum_{\log(n+1) \geqq m} \frac{1}{n^2} = O(1) \sum_{m=0}^{\infty} A_m < \infty,^{2})$$

woraus sich durch Anwendung des B. Levischen Satzes die Gültigkeit von (2) in $[a, b]$ fast überall ergibt.

Notwendigkeit. Wir nehmen an, (3) sei für eine Zahlenfolge $\{a_k\}$ nicht richtig und werden dann eine Orthogonalreihe mit den Koeffizienten a_k konstruieren, die fast überall nicht $|C, 1|$-summierbar ist. Ohne Beschränkung der Allgemeinheit kann $a_k = 0$ $(0 \leqq k \leqq 16)$, $a_k \geqq 0$ $(k > 16)$ und $[a, b] = [0, 1]$ gewählt werden. Es seien b_k rationale Zahlen mit $b_k = 0$ $(0 \leqq k \leqq 16)$, $0 < c_k = b_k - a_k \leqq k^{-2}$ $(k > 16)$. Da

$$B_m = (b_{2^m+1}^2 + \cdots + b_{2^{m+1}}^2)^{1/2} \geqq A_m \qquad (m = 0, 1, \ldots)$$

gilt, so ist nach (3)

$$\sum_{m=1}^{\infty} B_m = \infty. \tag{4}$$

Wir definieren zwei Folgen von natürlichen Zahlen $\{M(\mu)\}$ $(1 = M(0) < \cdots < M(\mu) < \cdots)$ und $\{m(\mu)\}$ $(0 \leqq m(\mu) \leqq 3;\ \mu = 1, 2, \ldots)$ mit der folgenden

---

2) $[\log(n+1)]$ bezeichnet den ganzen Teil von $\log(n+1)$.

Eigenschaft: für jede natürliche Zahl μ ($\geqq 1$) gilt

$$4\sum_{m=1}^{4M(\mu-1)-1} B_m \leqq \sum_{\nu=M(\mu-1)}^{M(\mu)-2} B_{4\nu+m(\mu)}. \tag{5}$$

Es seien nämlich $M(0)=1$, $M(1)=3$ und $m(1)=0$. Offensichtlich besteht dann (5) für $\mu=1$. Es sei ferner μ_0 ($\geqq 1$) eine natürliche Zahl. Wir nehmen an, $M(\mu)$ $(0\leqq\mu\leqq\mu_0)$ und $m(\mu)$ $(0\leqq m(\mu)\leqq 3)$ $(1\leqq\mu\leqq\mu_0)$ seien schon derart definiert, daß (5) für $\mu=1,\ldots,\mu_0$ besteht. Wegen (4) ist

$$\sum_{m=4M(\mu_0)}^{\infty} B_m=\infty,$$

daher gibt es einen Index $m(\mu_0+1)$ $(0\leqq m(\mu_0+1)\leqq 3)$, so daß

$$\sum_{\nu=M(\mu_0)}^{\infty} B_{4\nu+m(\mu_0+1)}=\infty$$

ist. Es sei $M(\mu_0+1)$ $(\geqq M(\mu_0)+2)$ die kleinste natürliche Zahl, für die

$$4\sum_{m=4}^{4M(\mu_0)-1} B_m \leqq \sum_{\nu=M(\mu_0)}^{M(\mu_0+1)-2} B_{4\nu+m(\mu_0+1)}$$

gilt. Dann ist (5) auch für $\mu=\mu_0+1$ erfüllt und damit die Folgen $\{M(\mu)\}$ und $\{m(\mu)\}$ mit den erwähnten Eigenschaften durch Induktion definiert.

Für jedes μ ($\geqq 1$) wird die Menge der Indizes $4M(\mu-1)+m(\mu)$, $4(M(\mu-1)+1)+m(\mu),\ldots,4(M(\mu)-2)+m(\mu)$ mit $J'(\mu)$ bezeichnet und $J''(\mu)$ bedeutet die Menge der Indizes m, für die $4M(\mu-1)\leqq m<4M(\mu)$ und $m\notin J'(\mu)$ erfüllt sind.

Es wird nun ein im Intervall $[0,1]$ orthonormiertes System von Treppenfunktionen $\Phi_k(x)$ $(k=0,1,\ldots)$ und eine Folge von einfachen Mengen $F_\mu(\subseteq[0,1])$ $(\mu=1,2,\ldots)$ definiert,[3]) für welche die folgenden Bedingungen erfüllt sind:

Die Mengen F_μ sind stochastisch unabhängig und für jedes μ gilt

$$\mathrm{mes}\,(F_\mu)=\frac{1}{2}\text{ [4])}; \tag{6}$$

die Abschätzung

$$b_{2^{m_{+1}}}|\Phi_{2^{m_{+1}}}(x)|+\cdots+b_{2^{m+1}}|\Phi_{2^{m+1}}(x)|\leqq\sqrt{2}\,B_m \qquad (0\leqq x\leqq 1) \tag{7}$$

[3]) D. h. für jedes $\Phi_k(x)$ kann das Intervall $[0,1]$ in endlich viele Teilintervalle zerlegt werden, derart, daß $\Phi_k(x)$ in jedem Teilintervall konstant ist; jede Menge F_μ ist die Vereinigung endlich vieler Intervalle.

[4]) Mit $\mathrm{mes}\,(H)$ wird das Lebesguesche Maß der Menge H bezeichnet.

besteht für jedes m ($\geqq 4$); ferner gelten die folgenden Beziehungen:

$$(8) \qquad b_{2^{m}+1}|\Phi_{2^{m}+1}(x)|+\cdots+b_{2^{m+1}}|\Phi_{2^{m+1}}(x)| = \sqrt{2}\,B_m \qquad (x\in F_\mu;\ m\in J'(\mu)),$$

$$(9) \qquad \Phi_k(x)\,\Phi_l(x)=0 \qquad (x\in F_\mu;\ k\neq l,\ 2^m<k,\ l\leqq 2^{m+1},\ m\in J'(\mu)),$$

außerdem

$$(10) \qquad \Phi_k(x)=0 \qquad (x\in F_\mu;\ 2^m<k\leqq 2^{m+1},\ m\in J''(\mu)).$$

Es seien $\Phi_k(x)=r_k(x)$ $(k=0,\ldots,16=2^{4M(0)})$, wo $r_k(x)=\operatorname{sign}\sin 2^k\pi x$ die k-te Rademachersche Funktion bedeutet. Diese sind Treppenfunktionen und bilden in $[0,1]$ ein orthonormiertes Funktionensystem.

Es sei μ_0 ($\geqq 1$) eine natürliche Zahl. Wir nehmen an, daß die Treppenfunktionen $\Phi_k(x)$ $(0\leqq k\leqq 2^{4M(\mu_0-1)})$ und die einfachen Mengen F_μ $(1\leqq\mu\leqq\mu_0-1)$ schon definiert sind, derart, daß diese Funktionen in $[0,1]$ ein orthonormiertes System bilden, die Mengen $F_1,\ldots,F_{\mu_0-1}$ stochastisch unabhängig sind, die Abschätzung (7) für $m=4,\ldots,4M(\mu_0-1)-1$ und die Beziehungen (8)—(10) für $\mu=1,\ldots,\mu_0-1$ erfüllt sind.

Dann kann das Intervall $[0,1]$ in endlich viele Teilintervalle $I(r)$ $(1\leqq r\leqq\varrho)$ eingeteilt werden, derart, daß in den einzelnen Teilintervallen $I(r)$ jede Funktion $\Phi_k(x)$ $(0\leqq k\leqq 2^{4M(\mu_0-1)})$ konstant ist und jede Menge F_μ $(1\leqq\mu\leqq\mu_0-1)$ die Vereinigung einiger $I(r)$ ist. Mit $I'(r)$ bzw. $I''(r)$ werden die zwei Hälften des Intervalls $I(r)$ bezeichnet. Wir schreiben die rationalen Zahlen $\frac{b_k^2}{B_m^2}$ $(2^m<k\leqq 2^{m+1},\ 4M(\mu_0-1)\leqq m<4M(\mu_0))$ als Brüche natürlicher Zahlen mit gemeinsamem Nenner auf: $\frac{b_k^2}{B_m^2}=\frac{p_k}{q(\mu_0)}$ und teilen jedes Intervall $I'(r)$ in $q(\mu_0)$ Teilintervalle gleicher Länge: $I'(r,i,\mu_0)$ $(1\leqq i\leqq q(\mu_0))$. Es sei

$$(11) \qquad \Phi_k(x)=\sqrt{2}\,\frac{B_m}{b_k}\sum_{r=1}^{\varrho}\ \sum_{i=p_{2^m+1}+\cdots+p_k-1+1}^{p_{2^m+1}+\cdots+p_k} r_m(x;\,I'(r,i,\mu_0))\ ^{5})$$

für $2^m<k\leqq 2^{m+1}$ mit $m\in J'(\mu_0)$. Ähnlich teilen wir auch jedes Intervall $I''(r)$ in $q(\mu_0)$ Teilintervalle gleicher Länge: $I''(r,i,\mu_0)$ $(1\leqq i\leqq q(\mu_0))$ und setzen

$$(12) \qquad \Phi_k(x)=\sqrt{2}\,\frac{B_m}{b_k}\sum_{r=1}^{\varrho}\ \sum_{i=p_{2^m+1}+\cdots+p_{k-1}+1}^{p_{2^m+1}+\cdots+p_k} r_m(x;\,I''(r,i,\mu_0))$$

---

5) Ist $I=[u,v]$ ein endliches Intervall und $f(x)$ eine in $[0,1]$ definierte Funktion, so sei $f(x;I)=f\left(\frac{x-u}{v-u}\right)$ für $u<x<v$ und $f(x;I)=0$ sonst. Offensichtlich gilt für jede in $[0,1]$ quadratisch integrierbare Funktion $f(x)$ und $g(x)$:

$$\int_u^v f(x;I)g(x;I)\,dx=\operatorname{mes}(I)\int_0^1 f(x)g(x)\,dx.$$

für $2^m < k \leqq 2^{m+1}$ mit $m \in J''(\mu_0)$. Es sei weiterhin F_{μ_0} die Menge, die aus der Vereinigung

$$\bigcup_{r=1}^{\varrho} I'(r)$$

nach Weglassen der endlich vielen Punkte zurückbleibt, in welchen die Funktionen $\Phi_k(x)$ $(2^{4M(\mu_0-1)} < k \leqq 2^{4M(\mu_0)})$ verschwinden.

Offensichtlich sind die Funktionen $\Phi_k(x)$ $(2^{4M(\mu_0-1)} < k \leqq 2^{4M(\mu_0)})$ Treppenfunktionen, die Menge F_{μ_0} ist einfach, die Funktionen $\Phi_k(x)$ $(0 \leqq k \leqq 2^{4M(\mu_0)})$ bilden in $[0, 1]$ ein orthonormiertes System und die Mengen $F_1, \ldots, F_{\mu_0}$ sind stochastisch unabhängig.

Da die Intervalle $I'(r)$ paarweise disjunkt sind und die Beziehungen

$$\operatorname{mes}(I'(r)) = \frac{1}{2}\operatorname{mes}(I(r)) \quad (1 \leqq r \leqq \varrho), \qquad \sum_{r=1}^{\varrho} \operatorname{mes}(I(r)) = 1$$

definitionsgemäß gelten, ist

$$\operatorname{mes}(F_{\mu_0}) = \sum_{r=1}^{\varrho} \operatorname{mes}(I'(r)) = \frac{1}{2}\sum_{r=1}^{\varrho} \operatorname{mes}((Ir)) = \frac{1}{2};$$

also wird (6) auch für $\mu = \mu_0$ erfüllt.

Es sei $m \in J'(\mu_0)$. Ist $x \in (0, 1)$, dann gilt $x \in I'(r, i, \mu_0)$ bzw. $x \in I''(r, i, \mu_0)$ nur für ein gewisses r und i. Nach (11) bzw. (12) ist dann die Summe $b_{2^m+1}|\Phi_{2^m+1}(x)| + \cdots + b_{2^{m+1}}|\Phi_{2^{m+1}}(x)|$ gleich $\sqrt{2}B_m|r_m(x; I'(r, i, \mu_0))| \leqq \sqrt{2}B_m$ bzw. $= 0$. Somit besteht (7) für $m \in J'(\mu_0)$. Ähnlich kann eingesehen werden, daß (7) auch für $m \in J''(\mu_0)$ besteht; also gilt (7) für jedes $m = 4M(\mu_0 - 1), \ldots, 4M(\mu_0) - 1$.

Ist $x \in F_{\mu_0}$, dann gilt $x \in I'(r, i, \mu_0)$ nur für ein gewisses r und i. Dann folgt für $m \in J'(\mu_0)$ aus (11) und aus der Definition von F_{μ_0}

$$b_{2^m+1}|\Phi_{2^m+1}(x)| + \cdots + b_{2^{m+1}}|\Phi_{2^{m+1}}(x)| = \sqrt{2}B_m|r_m(x; I'(r, i, \mu_0))| = \sqrt{2}B_m.$$

Also ist (8) für $\mu = \mu_0$ erfüllt.

Es sei $2^m < k \leqq 2^{m+1}$ mit $m \in J'(\mu_0)$. Nach (11) ist $\Phi_k(x) \neq 0$ nur in der Menge $E_k = \bigcup_{r=1}^{\varrho} \bigcup_{i=p_{2^m+1}+\ldots+p_{k-1}+1}^{p_{2^m+1}+\ldots+p_k} I'(r, i, \mu_0)$, ferner gilt $E_k \cap E_l = O$ für $2^m < k, l \leqq 2^{m+1}$, $k \neq l$, also ist (9) für $\mu = \mu_0$ erfüllt.

Es sei $2^m < k \leqq 2^{m+1}$ mit $m \in J''(\mu_0)$. Nach (12) ist $\Phi_k(x) = 0$ in der Menge $\bigcup_{r=1}^{\varrho} I'(r)$ $(\supseteq F_{\mu_0})$, woraus (10) für $\mu = \mu_0$ folgt.

Vollständige Induktion ergibt sodann ein unendliches Funktionensystem $\{\Phi_k(x)\}$ und eine unendliche Mengenfolge $\{F_\mu\}$ mit den erwähnten Eigenschaften.

Mit $\sigma_n^*(x)$ wird das n-te $(C,1)$-Mittel der Orthogonalreihe

$$\sum_{n=0}^{\infty} b_n \Phi_n(x)$$

bezeichnet.

Es sei $x \in F_\mu$ und $M(\mu-1) \leqq \nu < M(\mu)-2$. Dann ist

$$|\sigma^*_{2^{4(\nu+1)+m(\mu)}}(x) - \sigma^*_{2^{4\nu+m(\mu)}}(x)| \geqq$$

$$(13) \qquad \geqq \left| \sum_{k=2^{4\nu+m(\mu)}+1}^{2^{4(\nu+1)+m(\mu)}} \left(1 - \frac{k}{2^{4(\nu+1)+m(\mu)}+1}\right) b_k \Phi_k(x) \right| -$$

$$- \left| \sum_{k=17}^{2^{4\nu+m(\mu)}} \left(\frac{1}{2^{4\nu+m(\mu)}+1} - \frac{1}{2^{4(\nu+1)+m(\mu)}+1}\right) k b_k \Phi_k(x) \right| = S - R.$$

Wegen $x \in F_\mu$ folgt aus (10) $\Phi_k(x) = 0$ $(k = 2^{4\nu+m(\mu)+1}+1, \ldots, 2^{4(\nu+1)+m(\mu)})$ und daher ist

$$(14) \qquad S = \left| \sum_{k=2^{4\nu+m(\mu)}+1}^{2^{4\nu+m(\mu)+1}} \left(1 - \frac{k}{2^{4(\nu+1)+m(\mu)}+1}\right) b_k \Phi_k(x) \right|.$$

Da $x \in F_\mu$ und $4\nu + m(\mu) \in J'(\mu)$ gelten, folgt

$$(15) \qquad \left| \sum_{k=2^{4\nu+m(\mu)}+1}^{2^{4\nu+m(\mu)+1}} \left(1 - \frac{k}{2^{4(\nu+1)+m(\mu)}+1}\right) b_k \Phi_k(x) \right| =$$

$$= \sum_{k=2^{4\nu+m(\mu)}+1}^{2^{4\nu+m(\mu)+1}} \left(1 - \frac{k}{2^{4(\nu+1)+m(\mu)}+1}\right) b_k |\Phi_k(x)|$$

auf Grund von (9). Aus (14) und (15) folgt durch einfache Rechnung

$$S \geqq \frac{14}{16} \sum_{k=2^{4\nu+m(\mu)}+1}^{2^{4\nu+m(\mu)+1}} b_k |\Phi_k(x)|.$$

Da $x \in F_\mu$ und $4\nu + m(\mu) \in J'(\mu)$, ergibt sich auf Grund von (8):

$$(16) \qquad S \geqq \sqrt{2}\, \frac{14}{16} B_{4\nu+m(\mu)}.$$

Einfache Rechnung ergibt

$$R \leqq 16 \frac{1}{2^{4(\nu+1)+m(\mu)}} \sum_{m=4}^{4\nu+m(\mu)-1} 2^{m+1} \sum_{k=2^m+1}^{2^{m+1}} b_k |\Phi_k(x)|;$$

bei Beachtung von (10) und (7) folgt daraus

$$(17) \qquad R \leqq \frac{\sqrt{2}}{2^{4\nu}} \left(2^{4M(\mu-1)} \sum_{m=4}^{4M(\mu-1)-1} B_m + 2 \sum_{l=M(\mu-1)}^{\nu-1} 2^{4l} B_{4l+m(\mu)} \right).$$

Aus (13), (16) und (17) ergibt sich somit

$$\sum_{\nu=M(\mu-1)}^{M(\mu)-2} |\sigma^*_{2^{4(\nu+1)}+m(\mu)}(x) - \sigma^*_{2^{4\nu}+m(\mu)}(x)| \geqq$$

$$\geqq \sqrt{2}\left(\frac{14}{16}\sum_{\nu=M(\mu-1)}^{M(\mu)-2} B_{4\nu+m(\mu)} - 2\sum_{\nu=M(\mu-1)}^{M(\mu-2)}\frac{1}{2^{4\nu}}\sum_{l=M(\mu-1)}^{\nu-1} 2^{4l} B_{4l+m(\mu)} - \right. \tag{18}$$

$$\left. - \sum_{m=4}^{4M(\mu-1)-1} B_m 2^{4M(\mu-1)} \sum_{\nu=M(\mu-1)}^{M(\mu)-2}\frac{1}{2^{4\nu}}\right).$$

Es gilt aber

$$\sum_{\nu=M(\mu-1)}^{M(\mu)-2}\frac{1}{2^{4\nu}}\sum_{l=M(\mu-1)}^{\nu-1} 2^{4l} B_{4l+m(\mu)} =$$

$$= \sum_{l=M(\mu-1)}^{M(\mu)-3} B_{4l+m(\mu)} 2^{4l} \sum_{\nu=l+1}^{M(\mu)-2}\frac{1}{2^{4\nu}} \leqq \frac{1}{15}\sum_{\nu=M(\mu-1)}^{M(\mu)-2} B_{4\nu+m(\mu)} \tag{19}$$

und

$$\sum_{\nu=M(\mu-1)}^{M(\mu)-2}\frac{1}{2^{4\nu}} \leqq \frac{1}{2^{4M(\mu-1)}}\frac{16}{15}. \tag{20}$$

Aus (18), (19) und (20) folgt daher, daß

$$\sum_{\nu=M(\mu-1)}^{M(\mu)-2} |\sigma^*_{2^{4(\nu+1)}+m(\mu)}(x) - \sigma^*_{2^{4\nu}+m(\mu)}(x)| \geqq$$

$$\geqq \sqrt{2}\left(\frac{2}{3}\sum_{\nu=M(\mu-1)}^{M(\mu)-2} B_{4\nu+m(\mu)} - \frac{4}{3}\sum_{m=4}^{4M(\mu-1)-1} B_m\right)$$

für $x \in F_\mu$ gilt. Auf Grund von (5) ergibt sich, daß

$$\sum_{\nu=M(\mu-1)}^{M(\mu)-2} |\sigma^*_{2^{4(\nu+1)}+m(\mu)}(x) - \sigma^*_{2^{4\nu}+m(\mu)}(x)| \geqq \frac{\sqrt{2}}{3}\sum_{m=0}^{4M(\mu-1)-1} B_m \qquad (x \in F_\mu) \tag{21}$$

für jedes μ besteht.

Aus der stochastischen Unabhängigkeit der Mengen F_μ folgt wegen (6) durch Anwendung des zweiten Borel—Cantellischen Lemmas $\operatorname{mes}\left(\overline{\lim_{\mu\to\infty}} F_\mu\right) = 1$. Für $x \in F_\mu$ erhalten wir nach (21):

$$\sum_{n=0}^{2^{4M(\mu)}} |\sigma^*_{n+1}(x) - \sigma^*_n(x)| \geqq \sum_{n=2^{4M(\mu-1)+m(\mu)}}^{2^{4(M(\mu)-1)+m(\mu)-1}} |\sigma^*_{n+1}(x) - \sigma^*_n(x)| \geqq$$

$$\geqq \sum_{\nu=M(\mu-1)}^{M(\mu)-2} |\sigma^*_{2^{4(\nu+1)}+m(\mu)}(x) - \sigma^*_{2^{4\nu}+m(\mu)}(x)| \geqq \frac{\sqrt{2}}{3}\sum_{m=0}^{4M(\mu-1)-1} B_m.$$

Ist $x \in \overline{\lim_{\mu\to\infty}} F_\mu$, so gilt diese Abschätzung für unendlich viele μ, und mithin

gilt wegen (4)

$$\sum_{n=0}^{\infty} |\sigma_{n+1}^{*}(x) - \sigma_n^{*}(x)| = \infty, \tag{22}$$

also ist (22) in $[0, 1]$ fast überall erfüllt.

Mit $\sigma_n^{**}(x)$ wird das n-te $(C, 1)$-Mittel der Orthogonalreihe

$$\sum_{k=0}^{\infty} c_k \Phi_k(x)$$

bezeichnet. Nach der Definition der Konstanten c_k gilt

$$\sum_{m=0}^{\infty} (c_{2^m+1}^2 + \cdots + c_{2^{m+1}}^2)^{1/2} \leqq \sum_{k=0}^{\infty} c_k < \infty.$$

Auf Grund der Hinlänglichkeit der Bedingung (3) ist also

$$\sum_{n=0}^{\infty} |\sigma_{n+1}^{**}(x) - \sigma_n^{**}(x)| < \infty \tag{23}$$

fast überall in $[0, 1]$. Mit $\bar{\sigma}_n(x)$ wird das n-te $(C, 1)$-Mittel der Orthogonalreihe

$$\sum_{k=0}^{\infty} a_k \Phi_k(x) \tag{24}$$

bezeichnet. Da

$$\sum_{n=0}^{\infty} |\bar{\sigma}_{n+1}(x) - \bar{\sigma}_n(x)| \geqq \sum_{n=0}^{\infty} |\sigma_{n+1}^{*}(x) - \sigma_n^{*}(x)| - \sum_{n=0}^{\infty} |\sigma_{n+1}^{**}(x) - \sigma_n^{**}(x)|$$

ist, folgt aus (22) und (23), daß die Orthogonalreihe (24) in $[0, 1]$ fast überall nicht $|C, 1|$-summierbar ist.

Damit haben wir unseren Satz vollständig bewiesen.

(Eingegangen am 22. März 1960)

Eine Aufspaltung von Windung und Krümmung in affin zusammenhängenden Räumen

Von HANS REICHARDT in Berlin

L. Rédei zum 60. Geburtstag

Bei der Herleitung der Verallgemeinerungen der Frenetschen Formeln, des GAUSS'schen Theorema egregium und der Formeln von CODAZZI—MAINARDI in der Theorie der Teilräume n-dimensionaler Riemannscher Räume[1]) spielt die direkte Zerlegung des lokalen n-dimensionalen Vektorraumes, wie sie den Tangenten- und Schmiegräumen des Teilraumes entspricht, eine wesentliche Rolle. Im folgenden wird sich zeigen, daß man ein ganz ähnliches, nur wesentlich allgemeineres System von Formeln und Sätzen bekommt, wenn man in jedem Punkt einer Teilmannigfaltigkeit eines affin zusammenhängenden Raumes der Dimension n eine direkte Zerlegung des n-dimensionalen lokalen Vektorraumes vornimmt. Windung und Krümmung des ganzen Raumes spalten sich dann auf in „Krümmungstensoren", die zu den linearen Übertragungen gehören, die den einzelnen direkten Summanden entsprechen, sowie in infinitesimale Abbildungen, die jeden direkten Summanden in jeden anderen abbilden, und in gewisse alternierende Differentiale davon.

I. Interne Differentiation

Es sei $\mathfrak{A}$ ein affin zusammenhängender Raum und $\mathfrak{V}$ sein lokaler Vektorraum in einem beliebigen Punkte P von $\mathfrak{A}$. Ausgangspunkt für unsere Betrachtungen ist eine direkte Zerlegung von $\mathfrak{V}$:

$$\mathfrak{V} = \mathfrak{V}_1 \oplus \cdots \oplus \mathfrak{V}_k .$$

Jeder Vektor $\mathfrak{a} \in \mathfrak{V}$ besitzt dementsprechend eine eindeutige Zerlegung $\mathfrak{a} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_k$ mit $\mathfrak{a}_i \in \mathfrak{V}_i$. Der Übergang von $\mathfrak{a}$ zu einer Komponente ist eine lineare Abbildung N_i:

$$\mathfrak{a}_i = \mathsf{N}_i \mathfrak{a} .$$

[1]) Vgl. etwa H. REICHARDT, Zur Theorie der Teilräume Riemannscher Räume (Erscheint demnächst in der *Festschrift der Humboldt-Universität*, Berlin, 1960).

Die Bildung der Differentiale von Vektoren und Tensoren bezeichnen wir mit d. Die i-te Komponente des Differentials eines Vektors $\mathfrak{a}_j$ aus $\mathfrak{V}_j$ erscheint nun in zwei Gestalten, je nachdem, ob $i=j$ ist oder $i\neq j$, nämlich als eine „interne" Differentiation von $\mathfrak{V}_i$ („intern" soll andeuten, daß das Differential ganz in $\mathfrak{V}_i$ liegt) bzw. als infinitesimale lineare Abbildung von $\mathfrak{V}_j$ in $\mathfrak{V}_i$ („infinitesimal" soll andeuten, daß die Koordinaten der linearen Abbildung in Bezug auf irgendeine Basis Pfaffsche Formen sind). Die genannte Bildung $\mathsf{N}_i d\mathfrak{a}_j$ ist nämlich erstens auf jeden Fall additiv:

$$\mathsf{N}_i d(\mathfrak{a}_j+\mathfrak{b}_j)=\mathsf{N}_i d\mathfrak{a}_j+\mathsf{N}_i d\mathfrak{b}_j,$$

und zweitens gilt, wenn f eine skalare Ortsfunktion ist:

$$\mathsf{N}_i d(\mathfrak{a}_j f)=\mathsf{N}_i(d\mathfrak{a}_j\cdot f+\mathfrak{a}_j df)=(\mathsf{N}_i d\mathfrak{a}_j)f+(\mathsf{N}_i\mathfrak{a}_j)df.$$

Ist nun speziell $i=j$, so bekommt diese Formel die Gestalt einer Produktregel für eine Differentiation:

$$\mathsf{N}_i d(\mathfrak{a}_i f)=(\mathsf{N}_i d\mathfrak{a}_i)f+\mathfrak{a}_i df,$$

während für $i\neq j$ das Ergebnis

$$\mathsf{N}_i d(\mathfrak{a}_j f)=(\mathsf{N}_i d\mathfrak{a}_j)f$$

lautet. Schreiben wir dementsprechend einfach

$$\mathsf{N}_i d\mathfrak{a}_i=D\mathfrak{a}_i$$

(D hat also verschiedene Bedeutungen, je nachdem, aus welchem Summanden $\mathfrak{V}_i$ der zu differenzierende Vektor stammt) und

$$\mathsf{N}_i d\mathfrak{a}_j=\Omega_{ij}\mathfrak{a}_j \quad \text{für} \quad i\neq j,$$

so haben wir

$$\begin{aligned}
D(\mathfrak{a}_i+\mathfrak{b}_i)&=D\mathfrak{a}_i+D\mathfrak{b}_i,\\
D(\mathfrak{a}_i f)&=(D\mathfrak{a}_i)f+\mathfrak{a}_i df,\\
\Omega_{ij}(\mathfrak{a}_j+\mathfrak{b}_j)&=\Omega_{ij}\mathfrak{a}_j+\Omega_{ij}\mathfrak{b}_j,\\
\Omega_{ij}(\mathfrak{a}_j f)&=(\Omega_{ij}\mathfrak{a}_j)f.
\end{aligned}$$

Das heißt aber in der Tat, D, angewandt auf einen Vektor aus $\mathfrak{V}_i$, liefert ein in $\mathfrak{V}_i$ liegendes Differential (daher „internes" Differential), während Ω_{ij} eine lineare Abbildung von $\mathfrak{V}_j$ in $\mathfrak{V}_i$ bewirkt, deren Koordinaten auf Grund der Definition von Ω_{ij} Pfaffsche Formen sind.

Diese interne Differentiation der Vektorräume $\mathfrak{V}_i$ läßt sich nun ohne weiteres auf Tensorprodukte dieser Teilräume ausdehnen, indem man von dem im affin zusammenhängenden Raum $\mathfrak{A}$ definierten Differential des Tensors die jeweilige Komponente nimmt, d. h. z. B.: Ist $A\in\mathfrak{V}_i\otimes\mathfrak{V}_j\otimes\mathfrak{V}_h$, so

kann man A auch als Element von $\mathfrak{V}\otimes\mathfrak{V}\otimes\mathfrak{V}$ auffassen, daher dA als Element von $\mathfrak{V}\otimes\mathfrak{V}\otimes\mathfrak{V}$ bilden und diesen Tensor, der im allgemeinen nicht in $\mathfrak{V}_i\otimes\mathfrak{V}_j\otimes\mathfrak{V}_h$ liegen wird, durch Anwendung des Kronecker—Produktes der Projektionen von $\mathfrak{V}$ in diese Teilräume in ein Element von $\mathfrak{V}_i\otimes\mathfrak{V}_j\otimes\mathfrak{V}_h$ verwandeln: Durch

$$DA = (N_i\otimes N_j\otimes N_h)dA$$

wird somit eine interne Differentiation in $\mathfrak{V}_i\otimes\mathfrak{V}_j\otimes\mathfrak{V}_h$ definiert, und ganz entsprechend geht man vor bei beliebigen solchen „gemischten" Tensoren. Des weiteren lassen sich die Kovektorräume in diese interne Differentiation einbeziehen. Als Kovektorraum $\mathfrak{V}_i^*$ von $\mathfrak{V}_i$ nimmt man den Annulator von $\mathfrak{V}_1\oplus\cdots\oplus\mathfrak{V}_{i-1}\oplus\mathfrak{V}_{i+1}\oplus\cdots\oplus\mathfrak{V}_k$. Ist dann z. B. $A\in\mathfrak{V}_i^*\otimes\mathfrak{V}_j^*\otimes\mathfrak{V}_h$, so definiert man das interne Differential von A ganz entsprechend:

$$DA = (N_i^*\otimes N_j^*\otimes N_h)dA,$$

wobei N_i^* den Übergang von $\mathfrak{V}^*$ zu seiner $\mathfrak{V}_i^*$-Komponente bedeutet. Auf Grund dieser Definition beweist man ohne Mühe sofort die Produktregel für beliebige gemischte Tensoren:

$$D(A\otimes B) = DA\otimes B + A\otimes DB.$$

Im folgenden werden außer den gewöhnlichen Tensoren über $\mathfrak{V}_1,\ldots,\mathfrak{V}_m$, $\mathfrak{V}_1^*,\ldots,\mathfrak{V}_m^*$ auch noch infinitesimale vorkommen, und zwar solche, die man auffassen kann als Tensoren, deren Koordinaten bezüglich irgendeiner Basis alternierende Differentialformen der Stufe p sind, oder auch als alternierende Differentialformen der Stufe p, deren Koordinaten Tensoren irgendeines Typus sind. Für solche infinitesimalen Tensoren oder tensorielle Differentialformen ist ein Produkt (Operationszeichen $\circ$ [2]) etwa in der zweiten Auffassung so definiert, daß die tensoriellen Koordinaten tensoriell miteinander zu multiplizieren sind. Es ist dann z. B., wenn A und B gewöhnliche Tensoren beliebiger Typen und φ, χ alternierende Differentialformen beliebiger Stufen sind,

$$(A\varphi)\circ(B\chi) = (A\otimes B)\varphi\wedge\chi;$$

für gewöhnliche Tensoren reduziert sich dieses Produkt auf das tensorielle, $A\circ B = A\otimes B$, und für Differentialformen auf das äußere, $\varphi\circ\chi = \varphi\wedge\chi$.

Außerdem existiert für diese Gebilde ein äußeres Differential. Liegt z. B. Ω in $\mathfrak{V}_i\otimes\mathfrak{V}_j^*$, so ist Ω Summe von Produkten der Gestalt $A\omega$, wobei A ein gewöhnliches Element aus $\mathfrak{V}_i\otimes\mathfrak{V}_j^*$ und ω eine Differentialform der Stufe p ist. Dann gilt

$$d\wedge(A\omega) = (dA)\wedge\omega + Ad\wedge\omega.$$

[2]) Aus drucktechnischen Gründen wird hier das Zeichen $\circ$ verwendet anstelle des sonst von mir benützten, mit einem Kreis umgebenen $\wedge$.

Jedoch wird dieses Differential im allgemeinen kein Element von $\mathfrak{B}_i \otimes \mathfrak{B}_j^*$ mehr sein, sondern nur als Element von $\mathfrak{B} \otimes \mathfrak{B}^*$ aufgefaßt werden können. Zu einem internen, d. h. in $\mathfrak{B}_i \otimes \mathfrak{B}_j^*$ liegenden Differential kann man es nun machen, indem man das Kronecker-Produkt $N_i \otimes N_j^*$ darauf anwendet. Es wird daher definiert:

$$D \wedge \Omega = (N_i \otimes N_j^*) d \wedge \Omega.$$

Speziell ist also dann

$$D \wedge (A\omega) = (DA) \wedge \omega + A d \wedge \omega.$$

Aus der üblichen Produktregel folgt hier die entsprechende für das interne alternierende Differential:

$$D \wedge (\Omega_1 \circ \Omega_2) = (D \wedge \Omega_1) \circ \Omega_2 + (-1)^p \Omega_1 \circ D \wedge \Omega_2,$$

wobei p die Stufenzahl der (tensoriellen) Differentialform Ω_1 ist.

II. Die Ableitungsgleichungen und Integrabilitätsbedingungen

Ist dP das vektorielle Bogenelement in dem affin zusammenhängenden Raum $\mathfrak{A}$ und $e_1, \ldots, e_n$ eine Basis des lokalen Vektorraumes $\mathfrak{B}$ von P, so lauten die Ableitungsgleichungen (unter Beachtung der üblichen Summenkonvention)

$$dP = e_\varkappa \sigma^\varkappa, \tag{1}$$

wobei die $\sigma^\varkappa$ eine Basis der Pfaffschen Formen über $\mathfrak{A}$ bilden, sowie

$$d e_\lambda = e_\varkappa \tau^\varkappa{}_\lambda. \tag{2}$$

Bilden $\mathfrak{w}^1, \ldots, \mathfrak{w}^n$ die zu $e_1, \ldots, e_n$ duale Basis, so folgt in bekannter Weise

$$d\mathfrak{w}^\varkappa = -\tau^\varkappa{}_\lambda \mathfrak{w}^\lambda.$$

Die Grundgleichungen für $\mathfrak{A}$ lauten dann[3])

$$d \wedge \sigma^\varkappa + \tau^\varkappa{}_\lambda \wedge \sigma^\lambda = \omega^\varkappa, \tag{3}$$

$$d \wedge \tau^\varkappa{}_\lambda + \tau^\varkappa{}_\mu \wedge \tau^\mu{}_\lambda = \omega^\varkappa{}_\lambda, \tag{4}$$

wobei die $\omega^\varkappa$ und $\omega^\varkappa{}_\lambda$ die Koordinaten des Windungs- bzw. des Krümmungstensors von $\mathfrak{A}$ sind. Windung bzw. Krümmung fassen wir dabei als Vektor $t = e_\varkappa \omega^\varkappa$ bzw. als zweistufigen Tensor $K = e_\varkappa \otimes \mathfrak{w}^\lambda \omega^\varkappa{}_\lambda$ mit zweistufigen Differentialformen als Koordinaten auf. Es ist also

$$t = e_\varkappa (d \wedge \sigma^\varkappa + \tau^\varkappa{}_\lambda \wedge \sigma^\lambda), \tag{5}$$

$$K = e_\varkappa \otimes \mathfrak{w}^\lambda (d \wedge \tau^\varkappa{}_\lambda + \tau^\varkappa{}_\mu \wedge \tau^\mu{}_\lambda). \tag{6}$$

[3]) Vgl. etwa meine *Vorlesungen über Vektor- und Tensorrechnung* (Berlin, 1957), Kap. XI.

Es sei nun in jedem Punkt einer m-dimensionalen in $\mathfrak{A}$ gelegenen Fläche $\mathfrak{F}$ eine direkte Aufspaltung des lokalen Vektorraumes $\mathfrak{V}$ von $\mathfrak{A}$ gegeben:

$$\mathfrak{V} = \mathfrak{V}_1 \oplus \cdots \oplus \mathfrak{V}_k. \tag{7}$$

Für eine Basis von $\mathfrak{V}_1$ verwenden wir die Indizes α, β, γ, d. h. $\mathfrak{e}_\alpha$ durchläuft eine Basis von $\mathfrak{V}_1$, ebenso $\mathfrak{e}_\beta$ und auch $\mathfrak{e}_\gamma$, entsprechend $\mathfrak{e}_\iota, \mathfrak{e}_\varkappa, \mathfrak{e}_\lambda$ in $\mathfrak{V}_2$, $\mathfrak{e}_\mu, \mathfrak{e}_\nu, \mathfrak{e}_\varrho$ in $\mathfrak{V}_3, \ldots$.

Lassen wir P nur auf $\mathfrak{F}$ variieren, so spaltet sich die erste Ableitungsgleichung (1) auf in

$$dP = \mathfrak{e}_\alpha \sigma^\alpha + \mathfrak{e}_\iota \sigma^\iota + \mathfrak{e}_\mu \sigma^\mu + \cdots,$$

wobei die $\sigma^\alpha, \sigma^\iota, \sigma^\mu, \ldots$ Pfaffsche Formen über $\mathfrak{F}$ sind. Die Summenkonvention wird also für jedem Vektorraum $\mathfrak{V}_1, \mathfrak{V}_2, \mathfrak{V}_3, \ldots$ einzeln angewendet. Man kann dafür unter Benutzung der Projektionsoperatoren $\mathsf{N}_1, \mathsf{N}_2, \ldots$, die den Übergang von $\mathfrak{V}$ zu seinen Komponenten vermitteln, auch schreiben:

$$\mathsf{N}_1 dP = \mathfrak{e}_\alpha \sigma^\alpha, \quad \mathsf{N}_2 dP = \mathfrak{e}_\iota \sigma^\iota, \quad \mathsf{N}_3 dP = \mathfrak{e}_\mu \sigma^\mu, \ldots. \tag{8}$$

Ebenso spalten sich die übrigen Ableitungsgleichungen (2) in k Serien auf:

$$\begin{aligned} d\mathfrak{e}_\alpha &= \mathfrak{e}_\beta \tau^\beta{}_\alpha + \mathfrak{e}_\iota \tau^\iota{}_\alpha + \mathfrak{e}_\mu \tau^\mu{}_\alpha + \cdots, \\ d\mathfrak{e}_\iota &= \mathfrak{e}_\alpha \tau^\alpha{}_\iota + \mathfrak{e}_\varkappa \tau^\varkappa{}_\iota + \mathfrak{e}_\mu \tau^\mu{}_\iota + \cdots, \\ d\mathfrak{e}_\mu &= \mathfrak{e}_\alpha \tau^\alpha{}_\mu + \mathfrak{e}_\iota \tau^\iota{}_\mu + \mathfrak{e}_\nu \tau^\nu{}_\mu + \cdots, \quad \text{usw.} \end{aligned}$$

wofür man unter Benutzung des Zeichens D für die interne Differentiation und der Abbildungen Ω_{ij} von $\mathfrak{V}_j$ in $\mathfrak{V}_i$ auch schreiben kann:

$$\begin{aligned} &D\mathfrak{e}_\alpha = \mathfrak{e}_\beta \tau^\beta{}_\alpha, \quad \Omega_{21}\mathfrak{e}_\alpha = \mathfrak{e}_\iota \tau^\iota{}_\alpha, \quad \Omega_{31}\mathfrak{e}_\alpha = \mathfrak{e}_\mu \tau^\mu{}_\alpha, \ldots, \\ &\Omega_{12}\mathfrak{e}_\iota = \mathfrak{e}_\alpha \tau^\alpha{}_\iota, \quad D\mathfrak{e}_\iota = \mathfrak{e}_\varkappa \tau^\varkappa{}_\iota, \quad \Omega_{32}\mathfrak{e}_\iota = \mathfrak{e}_\mu \tau^\mu{}_\iota, \ldots, \\ &\Omega_{13}\mathfrak{e}_\mu = \mathfrak{e}_\alpha \tau^\alpha{}_\mu, \quad \Omega_{23}\mathfrak{e}_\mu = \mathfrak{e}_\iota \tau^\iota{}_\mu, \quad D\mathfrak{e}_\mu = \mathfrak{e}_\nu \tau^\nu{}_\mu, \ldots, \quad \text{usw.} \end{aligned} \tag{9}$$

Wählt man im Fall einer Kurve des n-dimensionalen euklidischen Raumes die direkte Zerlegung von $\mathfrak{V}$ in orthogonale Komponenten so, daß $\mathfrak{V}_1, \mathfrak{V}_1 \oplus \mathfrak{V}_2, \mathfrak{V}_1 \oplus \mathfrak{V}_2 \oplus \mathfrak{V}_3, \ldots$ den 1-dimensionalen Tangentenraum, den 2-, 3-, ..., -dimensionalen Schmiegraum bilden, so reduzieren sich diese Gleichungen auf die Frenetschen Formeln.

Weiter lassen sich jetzt die Abbildungen Ω_{ij} auf die Komponenten von $d\mathsf{N}_1, d\mathsf{N}_2, \ldots$ zurückführen. Es ist nämlich

$$\mathsf{N}_1 \mathfrak{e}_\alpha = \mathfrak{e}_\alpha, \quad \mathsf{N}_1 \mathfrak{e}_\iota = 0, \quad \mathsf{N}_1 \mathfrak{e}_\mu = 0, \ldots$$

also $N_1 = e_\alpha \otimes w^\alpha$, und daher

$$dN_1 = e_\beta \tau^\beta{}_\alpha \otimes w^\alpha + e_\iota \tau'{}_\alpha \otimes w^\alpha + e_\mu \tau^\mu{}_\alpha \otimes w^\alpha + \cdots$$
$$- e_\alpha \otimes \tau^\alpha{}_\beta w^\beta - e_\alpha \otimes \tau^\alpha{}_\iota w^\iota - e_\alpha \otimes \tau^\alpha{}_\mu w^\mu - \cdots .$$

Andererseits ist

$$\Omega_{12} e_\iota = N_1 d e_\iota = N_1 (e_\alpha \tau^\alpha{}_\iota + e_\varkappa \tau^\varkappa{}_\iota + \cdots) = e_\alpha \tau^\alpha{}_\iota$$

und daher

$$\Omega_{12} = e_\alpha \otimes w^\iota \tau^\alpha{}_\iota .$$

Ebenso gilt

$$\Omega_{13} = e_\alpha \otimes w^\mu \tau^\alpha{}_\mu ,$$
$$\cdots\cdots\cdots\cdots\cdots$$
(10) $$\Omega_{21} = e_\iota \otimes w^\alpha \tau'{}_\alpha ,$$
$$\Omega_{31} = e_\mu \otimes w^\alpha \tau^\mu{}_\alpha , \quad \text{usw.},$$

und daher geht die obige Formel für dN_1 über in

$$dN_1 = \Omega_{21} + \Omega_{31} + \cdots - \Omega_{12} - \Omega_{13} - \cdots .$$

Also ist

$$\Omega_{21} = (N_2 \otimes N_1^*) dN_1 ,$$
$$\Omega_{31} = (N_3 \otimes N_1^*) dN_1 ,$$
(11) $$\cdots\cdots\cdots\cdots\cdots$$
$$\Omega_{12} = -(N_1 \otimes N_2^*) dN_1 ,$$
$$\Omega_{13} = -(N_1 \otimes N_3^*) dN_1 , \quad \text{usw},$$

Mit Hilfe dieser Formeln können wir nun das Ergebnis der Aufspaltung der Integrabilitätsbedingungen invariant deuten. Die erste Serie (3) bekommt zunächst die Form

$$d \wedge \sigma^\alpha + \tau^\alpha{}_\beta \wedge \sigma^\beta + \tau^\alpha{}_\iota \wedge \sigma^\iota + \tau^\alpha{}_\mu \wedge \sigma^\mu + \cdots = \omega^\alpha ,$$
$$d \wedge \sigma' + \tau'{}_\alpha \wedge \sigma^\alpha + \tau'{}_\varkappa \wedge \sigma^\varkappa + \tau'{}_\mu \wedge \sigma^\mu + \cdots = \omega^\iota ,$$
$$d \wedge \sigma^\mu + \tau^\mu{}_\alpha \wedge \sigma^\alpha + \tau^\mu{}_\iota \wedge \sigma^\iota + \tau^\mu{}_\nu \wedge \sigma^\nu + \cdots = \omega^\mu ,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Nach (10) ist $\Omega_{12} = e_\alpha \otimes w^\iota \tau^\alpha{}_\iota$, also

$$\Omega_{12} \circ N_2 dP = (e_\alpha \otimes w^\iota \tau^\alpha{}_\iota) \circ (e_\varkappa \sigma^\varkappa) = e_\alpha \otimes w^\iota \otimes e_\varkappa \tau^\alpha{}_\iota \wedge \sigma^\varkappa .$$

Bezeichnen wir mit Y_ι die zu $\mathfrak{B}_\iota \otimes \mathfrak{B}_\iota^*$ gehörende Verjüngung, so gilt

$$Y_2(\Omega_{12} \circ N_2 dP) = e_\alpha \tau^\alpha{}_\iota \wedge \sigma^\iota ,$$

und setzen wir schließlich noch

$$\begin{aligned} t_1 &= \mathfrak{e}_\alpha(d \wedge \sigma^\alpha + \tau^\alpha{}_\beta \wedge \sigma^\beta), \\ t_2 &= \mathfrak{e}_\iota(d \wedge \sigma^\iota + \tau^\iota{}_\varkappa \wedge \sigma^\varkappa), \\ t_3 &= \mathfrak{e}_\mu(d \wedge \sigma^\mu + \tau^\mu{}_\nu \wedge \sigma^\nu), \quad \text{usw.}, \end{aligned} \tag{12}$$

so gehen die obigen Ableitungsgleichungen in die folgenden über:

$$\begin{aligned} &t_1 + Y_2(\Omega_{12} \circ N_2 dP) + Y_3(\Omega_{13} \circ N_3 dP) + \cdots = N_1 t, \\ &Y_1(\Omega_{21} \circ N_1 dP) + t_2 + Y_3(\Omega_{23} \circ N_3 dP) + \cdots = N_2 t, \\ &Y_1(\Omega_{31} \circ N_1 dP) + Y_2(\Omega_{32} \circ N_2 dP) + t_3 + \cdots = N_3 t, \quad \text{usw.}, \end{aligned} \tag{13}$$

aus denen die Koordinatenunabhängigkeit von $t_1, t_2, t_3, \ldots$ hervorgeht. Durch den Vergleich der Gleichung (5) mit den Gleichungen (12) wird man veranlaßt, $t_1, t_2, t_3, \ldots$ als die zu den Teilräumen $\mathfrak{B}_1, \mathfrak{B}_2, \mathfrak{B}_3, \ldots$ gehörenden Windungen zu bezeichnen.

Im GAUSS'schen Fall (Fläche im 3-dimensionalen euklidischen Raum) wird man $\mathfrak{B}_1$ als Menge der Tangentialvektoren und $\mathfrak{B}_2$ als Gesamtheit der Normalenvektoren nehmen. Dann tritt nur noch Ω_{12} auf, t, t_1 und t_2 werden zu 0, und die Gleichungen (13) liefern eine Symmetrieeigenschaft für Ω_{12}, deren Bedeutung man sich am einfachsten klar macht, wenn man in Ω_{12} die Basisdifferentiale σ^α durch die Basiskovektoren $\mathfrak{w}^\alpha$ ersetzt. Dann geht nämlich Ω_{12} in einen gewöhnlichen, im wesentlichen zweistufigen Tensor über. Dieser erweist sich dann (eben auf Grund der Gleichungen (13)) als symmetrisch, und seine charakteristischen Wurzeln und Hauptachsenrichtungen sind die Hauptkrümmungen und die Hauptkrümmungsrichtungen.

Addiert man die Gleichungen (13) zueinander, so ergibt sich

$$\sum_{i=1}^{k} t_i + \sum_{i \neq j} Y_i(\Omega_{ji} \circ N_i dP) = t,$$

woraus man umgekehrt durch Übergang zu den einzelnen Komponenten die sämtlichen Gleichungen (13) wieder zurückgewinnen kann.

In der gleichen Weise behandeln wir nun die zweite Serie (4) von Integrabilitätsbedingungen. Es entstehen dabei zwei verschiedene Typen von Gleichungen, die sich teils auf die interne Differentiation D, teils auf die Abbildungen Ω_{ij} beziehen. Zunächst ist

$$d \wedge \tau^\alpha{}_\beta + \tau^\alpha{}_\gamma \wedge \tau^\gamma{}_\beta + \tau^\alpha{}_\iota \wedge \tau^\iota{}_\beta + \tau^\varkappa{}_\mu \wedge \tau^\mu{}_\beta + \cdots = \omega^\alpha{}_\beta,$$

und weiter gilt

$$\begin{aligned} &Y_2(\Omega_{12} \circ \Omega_{21}) = Y_2((\mathfrak{e}_\alpha \otimes \mathfrak{w}^\iota \tau^\alpha{}_\iota) \circ (\mathfrak{e}_\varkappa \otimes \mathfrak{w}^\beta \tau^\varkappa{}_\beta)) \\ &= Y_2(\mathfrak{e}_\alpha \otimes \mathfrak{w}^\iota \otimes \mathfrak{e}_\varkappa \otimes \mathfrak{w}^\beta \tau^\alpha{}_\iota \wedge \tau^\varkappa{}_\beta) \quad = \mathfrak{e}_\alpha \otimes \mathfrak{w}^\beta \tau^\alpha{}_\iota \wedge \tau^\iota{}_\beta. \end{aligned}$$

Setzen wir also

$$\mathfrak{e}_\alpha \otimes \mathfrak{w}^\beta (d \wedge \tau^\alpha{}_\beta + \tau^\alpha{}_\gamma \wedge \tau^\gamma{}_\beta) = \mathsf{K}_1, \tag{14}$$

so ergibt sich

$$\mathsf{K}_1 + \mathsf{Y}_2(\Omega_{12} \circ \Omega_{21}) + \mathsf{Y}_3(\Omega_{13} \circ \Omega_{31}) + \cdots = (\mathsf{N}_1 \otimes \mathsf{N}_1^\dagger)\mathsf{K}, \tag{15}$$

und hieraus folgt, daß K_1 unabhängig von der Basiswahl ist. (Im GAUSS'schen Fall erkennt man leicht, daß diese Formel das Theorema egregium liefert.)

Der Tensor K_1 spielt eine Rolle, wenn man die zu der internen Differentiation von $\mathfrak{V}_1$ gehörende Übertragung untersucht. Ist nämlich längs einer auf unserer Fläche $\mathfrak{F}$ liegenden Kurve $\mathfrak{C}$ für einen dauernd in $\mathfrak{V}_1$ liegenden Vektor $\mathfrak{a}_1$ die Gleichung $D\mathfrak{a}_1 = 0$ erfüllt, so sagen wir, $\mathfrak{a}_1$ sei konstant auf $\mathfrak{C}$ oder werde längs $\mathfrak{C}$ übertragen. Man sieht, wie sonst üblich, leicht ein, daß diese Übertragung linear ist, d. h. daß sie einen ganz bestimmten Isomorphismus zwischen den zu den Punkten von $\mathfrak{C}$ gehörenden Vektorräumen $\mathfrak{V}_1$ vermittelt.

Das Ergebnis der Übertragung wird jedoch nicht nur von Anfangs- und Endpunkt, sondern vom ganzen Verlauf der Kurve $\mathfrak{C}$ abhängen. Überträgt man also einen Vektor aus $\mathfrak{V}_1$ längs einer von P ausgehenden geschlossenen Kurve $\mathfrak{C}$, so wird man im allgemeinen einen vom identischen verschiedenen Automorphismus des zu P gehörenden Vektorraumes $\mathfrak{V}_1$ erhalten. Nimmt man speziell für $\mathfrak{C}$ eine sehr kleine geschlossene Kurve, so wird dieser Automorphismus nur wenig vom identischen abweichen, und diese Abweichung wird in erster Näherung durch K_1 beschrieben, wobei in K_1 derjenige Bivektor einzusetzen ist, der dem umlaufenen Flächenelement entspricht. Man wird daher K_1 als den zu der in $\mathfrak{V}_1$ definierten linearen Übertragung gehörenden Krümmungstensor bezeichnen.

Geht man von der formelmäßigen Definition (14) von K_1 aus, so erhält man durch interne alternierende Differentiation nach kurzer Rechnung eine Formel, die im GAUSS'schen Fall, dort jedoch noch kombiniert mit einer von der Existenz der Metrik herrührenden Symmetrie, auf eine Verallgemeinerung der Identität von Bianchi führt, nämlich

$$\begin{aligned} D \wedge \mathsf{K}_1 &= 0, \\ D \wedge \mathsf{K}_2 &= 0, \\ D \wedge \mathsf{K}_3 &= 0, \quad \text{usw.} \end{aligned} \tag{16}$$

Den zweiten Typus von Gleichungen erhält man folgendermaßen: Es ist z. B.

$$d \wedge \tau^\alpha{}_\iota + \tau^\alpha{}_\beta \wedge \tau^\beta{}_\iota + \tau^\alpha{}_\varkappa \wedge \tau^\varkappa{}_\iota + \tau^\alpha{}_\mu \wedge \tau^\mu{}_\iota + \cdots = \omega^\alpha{}_\iota.$$

Nun ist

$$\begin{aligned} D \wedge \Omega_{12} &= D \wedge (\mathfrak{e}_\alpha \otimes \mathfrak{w}^\iota \tau^\alpha{}_\iota) \\ &= D(\mathfrak{e}_\alpha \otimes \mathfrak{w}^\iota) \wedge \tau^\alpha{}_\iota + \mathfrak{e}_\alpha \otimes \mathfrak{w}^\iota d \wedge \tau^\alpha{}_\iota \\ &= (D\mathfrak{e}_\alpha) \otimes \mathfrak{w}^\iota \wedge \tau^\alpha{}_\iota + \mathfrak{e}_\alpha \otimes (D\mathfrak{w}^\iota) \wedge \tau^\alpha{}_\iota + \mathfrak{e}_\alpha \otimes \mathfrak{w}^\iota d \wedge \tau^\alpha{}_\iota \\ &= \mathfrak{e}_\beta \tau^\beta{}_\alpha \otimes \mathfrak{w}^\iota \wedge \tau^\alpha{}_\iota - \mathfrak{e}_\alpha \otimes \tau^\iota{}_\varkappa \mathfrak{w}^\varkappa \wedge \tau^\alpha{}_\iota + \mathfrak{e}_\alpha \otimes \mathfrak{w}^\iota d \wedge \tau^\alpha{}_\iota \\ &= \mathfrak{e}_\alpha \otimes \mathfrak{w}^\iota (d \wedge \tau^\alpha{}_\iota + \tau^\alpha{}_\beta \wedge \tau^\beta{}_\iota + \tau^\alpha{}_\varkappa \wedge \tau^\varkappa{}_\iota). \end{aligned}$$

Also geht die obige Gleichung über in

$$D \wedge \Omega_{12} + Y_3(\Omega_{13} \circ \Omega_{32}) + \cdots = (N_1 \otimes N_2^*)K. \tag{17}$$

Diese Gleichung reduziert sich im GAUSS'schen Fall auf die Gleichungen von CODAZZI—MAINARDI.

Addiert man sämtliche Gleichungen vom Typ (15) und (17) zueinander, so erhält man

$$\sum_{i=1}^{k} K_i + \sum_{i \neq j} D \wedge \Omega_{ij} + \sum_{i \neq h \neq j}' Y_h(\Omega_{ih} \circ \Omega_{hj}) = K, \tag{18}$$

und aus dieser einzigen Gleichung kann man umgekehrt durch Übergang zu den einzelnen Komponenten die Verallgemeinerungen des Theorema egregium und der Formeln von CODAZZI—MAINARDI zurückgewinnen.

Nimmt man für $\mathfrak{A}$ den gewöhnlichen affinen Raum, so lassen sich Vektoren und Tensoren integrieren, da man sie jetzt auffassen kann als Vektoren und Tensoren des zu $\mathfrak{A}$ gehörenden n-dimensionalen Vektorraumes. Speziell kann man jetzt auf tensorielle alternierende Differentialformen den Stokesschen Satz anwenden. Schreibt man z. B. eine der Gleichungen, die die Formeln von CODAZZI—MAINARDI verallgemeinern, mit $d \wedge \Omega_{12}$ statt mit $D \wedge \Omega_{12}$, d. h. addiert man zu ihr $d \wedge \Omega_{12} - D \wedge \Omega_{12}$, so erhält man nach kurzer Rechnung

$$\begin{aligned} d \wedge \Omega_{12} &= (N_1 \otimes N_2^*)K \\ &+ Y_1((\Omega_{21} + \Omega_{31} + \cdots) \circ \Omega_{12}) + Y_2(\Omega_{12} \circ (\Omega_{21} + \Omega_{23} + \cdots)) \\ &- Y_3(\Omega_{13} \circ \Omega_{32}) - Y_4(\Omega_{14} \circ \Omega_{42}) - \cdots, \end{aligned}$$

und hieraus folgt nach dem Stokesschen Satz, angewandt auf ein zweidimensionales Flächenstück von $\mathfrak{F}$ und seinen Rand

$$\begin{aligned} \int \Omega_{12} = \iint \{ &(N_1 \otimes N_2^*)K + Y_1((\Omega_{21} + \Omega_{31} + \cdots) \circ \Omega_{12}) + \\ &+ Y_2(\Omega_{12} \circ (\Omega_{21} + \Omega_{23} + \cdots)) - Y_3(\Omega_{13} \circ \Omega_{32}) - Y_4(\Omega_{14} \circ \Omega_{42}) - \cdots \}. \end{aligned} \tag{19}$$

Entsprechende Formeln, gebildet mit Ω_{ij}, stellen dann ein gewisses Analogon zu dem Integralsatz von GAUSS—BONNET dar.

Eine weitere Serie von Integralsätzen läßt sich in entsprechender Weise aus (16) herleiten.

(Eingegangen am 31. März 1960)

Einfacher Beweis des Frobeniusschen Fundamentalsatzes der Gruppentheorie für den Fall eines quadratfreien Exponenten

Von HORST SACHS in Halle/Saale (Deutschland)

Professor L. Rédei zum 60. Geburtstag gewidmet

Der Satz von FROBENIUS besagt in seiner ursprünglichen Fassung:

Es seien $\mathfrak{G}$ eine endliche Gruppe der Ordnung g, n ein Teiler von g. Dann gilt: Die Anzahl N der Elemente X von $\mathfrak{G}$, welche der Gleichung $X^n = 1$ genügen, ist durch n teilbar.

Die bekannten Beweise sind, verglichen mit der einfachen Aussage des Satzes, recht kompliziert und wenig befriedigend. Es ist daher wohl der Mühe wert, nach neuen Beweismotiven zu suchen.[1])

Im Folgenden wird mittels elementar-kombinatorischer Methoden ein schwächerer Satz bewiesen, welcher immerhin im Falle eines quadratfreien Exponenten n dasselbe aussagt wie der Satz von FROBENIUS.

*

Satz. *Es seien $\mathfrak{G}$ eine endliche Gruppe der Ordnung g, n ein Teiler von g, p ein Primteiler von n. Dann gilt: Die Anzahl N der Elemente X von $\mathfrak{G}$, welche der Gleichung*

$$X^n = 1 \tag{1}$$

genügen, ist durch p teilbar.

Folgerung. *Ist n quadratfrei, so gilt: N ist durch n teilbar.*

Beweis. Die Gleichung

$$Y^{\frac{n}{p}} = 1 \tag{2}$$

habe in $\mathfrak{G}$ genau die r Lösungen $Y_1, \ldots, Y_r$ (es ist $r \geqq 1$, weil $Y = 1$ eine

[1]) Man vergleiche auch H. ZASSENHAUS, *Lehrbuch der Gruppentheorie.* I (Leipzig—Berlin, 1937 (Nachdruck 1948)), Seite 26: „*Der folgende Satz* [von FROBENIUS] *ist noch nicht in befriedigender Weise in einen größeren Zusammenhang gefügt.*“

Lösung von (2) ist). Die Gesamtheit der Lösungen X von (1) stimmt überein mit der Gesamtheit derjenigen X von $\mathfrak{S}$, welche einer der Gleichungen

$$X^p = Y_\varrho \qquad (\varrho = 1, \ldots, r)$$

genügen.

Es durchlaufe A_i $(i = 1, \ldots, g)$ die sämtlichen Elemente der Gruppe $\mathfrak{S}$. Wir betrachten die Gesamtheit der geordneten $(p-1)$-tupel

$$T_{i_1 \ldots i_{p-1}} = \{A_{i_1}, \ldots, A_{i_{p-1}}\},$$

wo die Indizes unabhängig voneinander die Werte $1, \ldots, g$ durchlaufen; ihre Anzahl ist g^{p-1}. Zu jedem solchen $(p-1)$-tupel sind durch die Bedingungen $A_{i_1} A_{i_2} \ldots A_{i_{p-1}} A_{i_p} = Y_\varrho$ $(\varrho = 1, \ldots, r)$ genau r verschiedene (von $T_{i_1 \ldots i_{p-1}}$ und ϱ abhängende) Elemente A_{i_p} bestimmt. Wir betrachten nun die Menge $\mathfrak{M}$ der so entstandenen geordneten p-tupel

$$\{A_{i_1}, \ldots, A_{i_p}\};$$

sie sind paarweise verschieden, ihre Anzahl ist $M = r \cdot g^{p-1}$. In $\mathfrak{M}$ sind alle geordneten p-tupel $\{A_{j_1}, \ldots, A_{j_p}\}$ und nur solche mit der Eigenschaft

$$A_{j_1} \ldots A_{j_p} = Y_\varrho \qquad (\varrho = 1, \ldots, r)$$

enthalten.

Die Anzahl N ist offenbar gleich der Anzahl derjenigen p-tupel von $\mathfrak{M}$, die lauter gleiche Elemente enthalten; diese bilden eine Untermenge $\mathfrak{N}$ von $\mathfrak{M}$. Wir haben

$$p \mid r \cdot g^{p-1} = M = N + (M - N);$$

können wir nun zeigen, daß $p \mid M - N$, so folgt $p \mid N$, und das ist gerade die zu beweisende Behauptung.

$M - N$ ist die Anzahl der p-tupel von $\mathfrak{M} - \mathfrak{N}$, also die Anzahl derjenigen p-tupel von $\mathfrak{M}$, welche mindestens zwei verschiedene Elemente enthalten.

Durch zyklische Umordnung der Elemente eines p-tupels von $\mathfrak{M} - \mathfrak{N}$ entstehen wieder p-tupel von $\mathfrak{M} - \mathfrak{N}$, denn aus $A_{i_1} \ldots A_{i_p} = Y$ mit $Y^{\overset{n}{p}} = 1$ folgt $A_{i_p} A_{i_1} \ldots A_{i_{p-1}} = A_{i_p} Y A_{i_p}^{-1} = Z$ mit $Z^{\overset{n}{p}} = 1$ usw.; auf diese Weise gewinnen wir aus einem p-tupel von $\mathfrak{M} - \mathfrak{N}$ genau p offenbar paarweise verschiedene p-tupel von $\mathfrak{M} - \mathfrak{N}$. Die Menge $\mathfrak{M} - \mathfrak{N}$ zerfällt so in (elementfremde) Klassen zyklisch-äquivalenter p-tupel, deren jede genau p p-tupel enthält. Folglich ist $M - N$ durch p teilbar. Das war zu zeigen.

(Eingegangen am 14. April 1960)

A theorem on diophantine approximation with application to Riemann zeta-function

By P. TURÁN in Budapest

To the sixtieth birthday of my friend Prof. L. Rédei

1. In a recent paper[1]) I proved among others the following theorem. If for $n > n_0$ none of the Dirichlet-polynomials

$$U_n(s) = \sum_{\nu \leqq n} \nu^{-s} \qquad (s = \sigma + it) \tag{1}$$

vanishes in a half-strip

$$\sigma \geqq 1 + \frac{\log^3 n}{\sqrt{n}}, \quad \gamma_n \leqq t \leqq \gamma_n + e^{n^3} \tag{1.2}$$

with a suitable real γ_n, then RIEMANN's conjecture is true.

Also a sort of converse theorems was proved in the above quoted paper. The aim of the present note is to improve the above quoted theorem by proving that *Riemann's conjecture follows even from the weaker assumption that for $n > n_0$ the polynomials $U_n(s)$ do not vanish in the half-strip*

$$\sigma \geqq 1 + \frac{\log^3 n}{\sqrt{n}}, \quad \gamma_n \leqq t \leqq \gamma_n + e^{n^{\frac{1}{2}}} \tag{1.3}$$

with a suitable real γ_n.

Probably the half-strip (1.3) could be replaced in the theorem by the half-strip

$$\sigma \geqq 1 + \frac{\log^3 n}{\sqrt{n}}, \quad \gamma_n \leqq t \leqq \gamma_n + e^{c_1 n} \tag{1.4}$$

with a suitable c_1, where c_1 — and later $c_2, c_3, \ldots$ — stand for positive numerical constants.

---

[1]) P. TURÁN, Nachtrag zu meiner Abhandlung "On some approximative Dirichlet polynomials in the theory of zeta-function of Riemann", *Acta Math. Acad. Sci. Hung.*, 10 (1959), 277—298.

Again an infinite number of exceptional polynomials $U_n(s)$ vanishing in *every* half-strip of the form (1.3), could have been admitted, supposing that the number of such indices not exceeding x is $o(\log x)$ for $x \to \infty$. We shall omit this as well as the similar theorems for

$$C_n(s) = \sum_{\nu \leqq n} \left(1 - \frac{\nu}{n+1}\right) \nu^{-s}, \quad V_n(s) = \sum_{\nu \leqq n} (-1)^{\nu+1} \nu^{-s},$$

$$W_n(s) = \sum_{\nu \leqq n} (-1)^{\nu} (2\nu - 1)^{-s}$$

and the proof that $U_n(s)$ does not vanish for $n > c_2$ in the domain

$$\sigma \geqq 1, \quad c_3 \leqq t \leqq e^{c_4 \log^{\frac{1}{2}} n}. \tag{1.5}$$

But I do emphasize again as I did in my above quoted paper two facts. First that in order to verify the condition in (1.3) it would suffice to prove

$$\lim_{T \to \infty} \frac{N_n(T)}{T} < e^{-n^{\frac{1}{2}}} \tag{1.6}$$

where $N_n(T)$ stands for the number of zeros of $U_n(s)$ for

$$\sigma \geqq 1 + \frac{\log^3 n}{\sqrt{n}}, \quad 0 \leqq t \leqq T \tag{1.7}$$

and for which to prove e. g. the inequality

$$N_n(T) < c_5 \frac{T}{n}$$

is easy. Secondly though the proofs work "essentially" also for all functions $f(s)$ which are representable for $\sigma > 1$ by an absolutely convergent Dirichlet-series

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

with positive monotonical coefficients a_n and also by an Euler-product

$$\prod_p \frac{1}{1 - \frac{b_p}{p^s}} \qquad (b_p \text{ real}),$$

these three properties already *characterize* $\zeta(s)$ up to a translation of s, perhaps surprisingly for the first minute, owing to the existing big literature of the characterisation-problem.

2. The improvement is furnished by a lemma which belongs to the theory of diophantine approximation; a theory to which RÉDEI made valuable contributions. This will be the

L e m m a. *If* $2 = p_1 < p_2 < \cdots < p_N$ *stand for the first* N *primes,* $d, \beta_1, \beta_2, \ldots, \beta_N$ *for arbitrary real numbers and* ω *is an integer* $\geqq 4$, *then there is a* t_0 *with*

$$d \leqq t_0 \leqq d + e^{17\omega N \log^3 N} \tag{2.1}$$

such that for $\nu = 1, 2, \ldots, N$ *the inequalities*

$$|t_0 \log p_\nu - \beta_\nu - e_\nu| \leqq \frac{1}{\omega} \qquad (e_\nu \text{ integers}) \tag{2.2}$$

hold[2]*), if only* $N > c_6 (> e^{31})$, $N > \omega$.

The half-strip (1.3) could be replaced by the one in (1.4) if the interval in (2.1) could have been replaced by

$$d \leqq t_0 \leqq d + \omega^N$$

say (which would be essentially best-possible).

For the proof of the lemma we make first some preparations. Let

$$k = [\log N] \ (\geqq 30), \quad m = [e^2 \omega] \ (> 4), \tag{2.3}$$

$$A = \int_0^1 \left(\frac{\sin m\pi x}{\sin \pi x} \right)^{2k} dx, \tag{2.4}$$

and

$$P(x) = \frac{1}{A} \cdot \left(\frac{\sin m\pi x}{\sin \pi x} \right)^{2k}. \tag{2.5}$$

Since after FEJÉR's formula we have

$$\frac{1}{m} \left(\frac{\sin m\pi x}{\sin \pi x} \right)^2 = \sum_{\nu=-(m-1)}^{m-1} \left(1 - \frac{|\nu|}{m} \right) e^{2\pi i \nu x},$$

we get

$$P(x) = \sum_{\nu=-(m-1)k}^{(m-1)k} a'_\nu e^{2\pi i \nu x} \tag{2.6}$$

with positive a'_ν satisfying

$$a'_{-\nu} = a'_\nu \quad \text{and} \quad a'_0 = 1. \tag{2.7}$$

---

[2]) In the previous form the exponent in (2.1) was $3(N\omega)^2 \log^2 N\omega$.

It is easy to verify from (2.6) and (2.5) that

$$\sum_{\nu=-(m-1)k}^{(m-1)k} a'_\nu z^\nu = \frac{1}{A} z^{-(m-1)k} \left(\frac{z^m-1}{z-1}\right)^{2k}. \tag{2.8}$$

Finally we shall need the simple inequality from (2.4)

$$A > \int_0^1 \left(\frac{\sin m\pi x}{\pi x}\right)^{2k} dx = \frac{1}{\pi} m^{2k-1} \int_0^{m\pi} \left(\frac{\sin t}{t}\right)^{2k} dt >$$

$$> \frac{m^{2k-1}}{\pi} \int_0^{k^{-\frac{1}{3}}} \left(\frac{\sin t}{t}\right)^{2k} dt > \frac{m^{2k-1}}{3\pi\sqrt{k}}$$

i. e.

$$A > \frac{m^{2k-1}}{3\pi\sqrt{k}} \tag{2.9}$$

(and obviously $\geqq 2$).

3. Let

$$T = e^{17\omega N \log^3 N} \tag{3.1}$$

and modifying an idea of H. BOHR and B. JESSEN[3]) devised by them for the proof of KRONECKER's theorem we consider the function

$$K_N(t) = \prod_{j=1}^{N} P(t \log p_j - \beta_j) \tag{3.2}$$

with fixed β_j. If the lemma would be false then for all $d \leqq t \leqq d+T$ for a suitable index $\nu = \nu(t)$ we would have

$$|t \log p_\nu - \beta_\nu - e_\nu| > \frac{1}{\omega}$$

for all integer e_ν and thus, using also (2.3), (2.9) and (2.5),

$$(0 \leqq) P(t \log p_\nu - \beta_\nu) < \frac{1}{A} \frac{1}{\sin^{2k} \frac{\pi}{\omega}} < \frac{3\pi\sqrt{k}}{m^{2k-1}} \cdot \frac{1}{\sin^{2k} \frac{\pi}{\omega}} <$$

$$< \frac{3\pi e^2 \omega \sqrt{\log N}}{\left(\frac{2m}{\omega}\right)^{2k}} < \frac{3\pi e^6 \omega \sqrt{\log N}}{N^4} < \frac{3\pi e^6 \sqrt{\log N}}{N^3} < \frac{1}{N^2}, \tag{3.3}$$

[3]) H. BOHR—B. JESSEN, Zum Kroneckerschen Satz, *Rendiconti del Circolo Mat. Palermo*, **57** (1933), 123—129.

if c_6 is sufficiently large. Hence for this t we had

$$K_N(t) < \frac{1}{N^2} \prod_{\substack{j=1 \\ j \neq \nu}}^{N}{}' P(t \log p_j - \beta_j) \overset{\text{def}}{=} \frac{1}{N^2} K_{N\nu}(t)$$

and thus owing to the nonnegativity of $P(x)$

$$K_N(t) < \frac{1}{N^2} \sum_{\nu=1}^{N} K_{N\nu}(t)$$

would hold throughout $[0, T]$. Integrating we would obtain

$$J_N \overset{\text{def}}{=} \int_a^{a+T} K_N(t)\,dt < \frac{1}{N^2} \sum_{\nu=1}^{N} \int_a^{a+T} K_{N\nu}(t)\,dt \overset{\text{def}}{=} \frac{1}{N^2} \sum_{\nu=1}^{N} J_{N\nu}. \tag{3.4}$$

4. In order to deduce a contradiction from (3.4) we have to estimate J_N and the $J_{N\nu}$'s. To do it simultaneously let

$$q_1, q_2, \ldots, q_r \qquad 1 \leqq r \leqq N$$

be r different primes, $\gamma_1, \gamma_2, \ldots, \gamma_r$ real,

$$G_r(t) = \prod_{j=1}^{r} P(t \log q_j - \gamma_j) \tag{4.1}$$

and

$$\int_a^{a+T} G_r(t)\,dt = H_r. \tag{4.2}$$

Then (2.6) gives owing to the rational independence of the $\log q_j$'s and (2.7)

$$G_r(t) = 1 + \sum_{\substack{-(m-1)k \leqq \nu_j \leqq (m-1)k \\ j=1,2,\ldots,r}} a'_{\nu_1} a'_{\nu_2} \ldots a'_{\nu_r} e^{-2\pi i(\nu_1\gamma_1 + \cdots + \nu_r\gamma_r)} e^{2\pi i t \log\left(q_1^{\nu_1} q_2^{\nu_2} \cdots q_r^{\nu_r}\right)}$$

and thus with a ϑ, $-\frac{1}{\pi} \leqq \vartheta \leqq \frac{1}{\pi}$,

$$H_r = T + \vartheta \sum_{\substack{-(m-1)k \leqq \nu_j \leqq (m-1)k \\ j=1,2,\ldots,r}} \frac{a'_{\nu_1} a'_{\nu_2} \ldots a'_{\nu_r}}{\left|\log\left(q_1^{\nu_1} q_2^{\nu_2} \ldots q_r^{\nu_r}\right)\right|} \overset{\text{def}}{=} T + \vartheta Z. \tag{4.3}$$

In order to obtain an upper bound for Z we consider first with an l, $1 \leqq l \leqq r$, the partial sum

$$Z_{j_1 j_2 \ldots j_l} \qquad (1 \leqq j_1 < \cdots < j_l \leqq r)$$

of Z, consisting of the terms where exactly the summation variables

$\nu_{j_1}, \nu_{j_2}, \ldots, \nu_{j_l}$ have values different from 0. Hence owing to (2.7) we have

$$(4.4)\quad Z_{j_1 j_2 \ldots j_l} = \sum_{\substack{1 \leqq \varkappa_i \leqq (m-1)k \\ (i=1,\ldots,l)}} a'_{\varkappa_1} a'_{\varkappa_2} \ldots a'_{\varkappa_l} \sum_{\substack{\varepsilon_i = \pm 1 \\ (i=1,\ldots,l)}} \frac{1}{|\log (q_{j_1}^{\varepsilon_1 \varkappa_1} q_{j_2}^{\varepsilon_2 \varkappa_2} \ldots q_{j_l}^{\varepsilon_l \varkappa_l})|}.$$

Since for integer $a > b \geqq 1$

$$\left|\log \frac{a}{b}\right| = \left|\log \frac{b}{a}\right| = \log\left(1 + \frac{a-b}{b}\right) > \frac{1}{2b},$$

we get for the inner sum in (4.4) at once the upper bound

$$2(1 + q_{j_1}^{\varkappa_1})(1 + q_{j_2}^{\varkappa_2}) \ldots (1 + q_{j_l}^{\varkappa_l}).$$

Putting this into (4.4) we get the inequality

$$Z_{j_1 j_2 \ldots j_l} < 2 \prod_{\mu=1}^{l} \left\{ \sum_{1 \leqq \varkappa_\mu \leqq (m-1)k} a'_{\varkappa_\mu} (1 + q_{j_\mu}^{\varkappa_\mu}) \right\} < 2 \prod_{\mu=1}^{l} \left\{ 2 \sum_{1 \leqq \varkappa_\mu \leqq (m-1)k} a'_{\varkappa_\mu} q_{j_\mu}^{\varkappa_\mu} \right\},$$

and thus

$$Z < 2 \prod_{\mu=1}^{r} \left\{ 1 + 2 \sum_{1 \leqq \varkappa_\mu \leqq (m-1)k} a'_{\varkappa_\mu} q_\mu^{\varkappa_\mu} \right\} < 2 \prod_{\mu=1}^{r} 2 \left\{ \sum_{-(m-1)k \leqq \varkappa_\mu \leqq (m-1)k} a'_{\varkappa_\mu} q_\mu^{\varkappa_\mu} \right\}.$$

Using the identity (2.8) this gives

$$Z < 2 \left(\frac{2}{A}\right)^r \frac{1}{(q_1 q_2 \ldots q_r)^{(m-1)k}} \prod_{\mu=1}^{r} \left(\frac{q_\mu^m - 1}{q_\mu - 1}\right)^{2k}$$

and roughly

$$(4.5)\quad Z < 2 (q_1 q_2 \ldots q_r)^{(m-1)k} \prod_{\mu=1}^{r} \frac{1 - \frac{1}{q_\mu^m}}{1 - \frac{1}{q_\mu}} < 20 (q_1 q_2 \ldots q_r)^{(m-1)k} e^{\sum_{\mu=1}^{r} q_\mu^{-1}}.$$

Applying it with

$$r = N, \quad (q_1, q_2, \ldots, q_r) = (p_1, p_2, \ldots, p_N), \quad \gamma_j = \beta_j$$

resp.

$$r = N-1, \quad (q_1, q_2, \ldots, q_r) = (p_1, p_2, \ldots, p_{\nu-1}, p_{\nu+1}, \ldots, p_N), \quad \gamma_j = \beta_j$$

$(\nu = 1, 2, \ldots, N)$ we get from (3.4), (4.3) and (4.5)

$$T - 7 (p_1 p_2 \ldots p_N)^{(m-1)k} e^{\sum_{\nu=1}^{N} p_\nu^{-1}} < \frac{1}{N^2} \left\{ NT + 7N (p_1 p_2 \ldots p_N)^{(m-1)k} e^{\sum_{\nu=1}^{N} p_\nu^{-1}} \right\}$$

i. e. roughly

$$\frac{1}{2} T < 11 (p_1 p_2 \ldots p_N)^{(m-1)k} e^{\sum_{\nu=1}^{N} p_\nu^{-1}}.$$

But as well-known, choosing c_6 sufficiently large, it follows

$$\frac{1}{2}T<11\log^2 N\cdot e^{2N\log N\cdot(m-1)k}<11\log^2 N e^{2e^2\omega N\log^2 N}.$$

Hence, if c_6 is large enough,

$$T<22\log^2 N\cdot e^{16\omega N\log^2 N}<e^{17\omega N\log^2 N},$$

in contradiction to (3. 1). Hence the lemma is proved.

5. Since the other parts of the proof are unchanged, as it is given in my above quoted paper, a sketch of it will suffice, for the sake of completeness. Let $\lambda(\nu)$ stand for LIOUVILLE's symbol, further for $n>c_7$

(5. 1) $$G_n(s)=\sum_{\nu\leqq n}\lambda(\nu)\nu^{-s}$$

and

(5. 2) $$\delta=\frac{\log^4 n}{\sqrt{n}};$$

we shall use the well-known estimation

(5. 3) $$|B(x)|\overset{\text{def}}{=}\left|\sum_{\nu\leqq x}\lambda(\nu)\right|<xe^{-c_8\sqrt{\log x}}.$$

With this c_8 (5. 3) gives easily that

(5. 4) $$|G_n(s)|<c_9$$

in the domain

$$\sigma\geqq 1-\frac{c_8}{3}\frac{1}{\sqrt{\log n}},\quad |t|\leqq 1,$$

if only n sufficiently large. Supposing now that $G_n(s)$ has a real zero σ_0 between $(1+2\delta)$ and $\left(1+3\frac{\log\log n}{\log n}\right)$ and putting

(5. 5) $$G_n(s)=\sum_{l=1}^{\infty}d_l\,(s-\sigma_0)^l,$$

CAUCHY's coefficient-estimation, applied to the circle

$$|s-\sigma_0|\leqq\frac{c_8}{8\sqrt{\log n}}$$

gives from (5. 4) the estimation

(5. 6) $$|d_l|<(c_9\log n)^{\frac{l}{2}}.$$

Further from

$$|d_1|=\left|\sum_{\nu\leqq n}\frac{\lambda(\nu)\log\nu}{\nu^{\sigma_0}}\right|,$$

from (5.3) and simple properties of $\zeta(s)$ we get the lower bound

$$|d_1| > \frac{1}{3}. \tag{5.7}$$

From (5.5), (5.6) and (5.7) we get the estimation

$$|G_n(s)| > \frac{\delta}{4} \tag{5.8}$$

on the circle $|s-\sigma_0| = \delta$. Application of the lemma with

$$N = \pi(n)\left(< 2\frac{n}{\log n}\right), \quad \beta_1 = \beta_2 = \cdots = \beta_{\pi(n)} = \frac{1}{2}, \quad \omega = \left[\frac{50\log^2 n}{\delta}\right] + 1$$

gives to every real d the existence of a τ_d with

$$d \leqq \tau_d \leqq d + e^{17\frac{51\sqrt{n}}{\log^2 n}\cdot 2\frac{n}{\log n}\cdot \log^2 n} \leqq d + \left(e^{n^{\frac{3}{2}}} - 1\right)\frac{1}{2\pi}$$

(if c_7 is large enough) such that

$$\left|\tau_d \log p - \frac{1}{2} - e_p\right| < \frac{\delta}{50\log^2 n} \quad (e_p \text{ integer})$$

for all $p \leqq n$. From this one can deduce that if c_7 is large enough than for $n > c_7$ and $\sigma \geqq 1$ we have

$$|G_n(s) - U_n(s + 2\pi i\tau_d)| < \frac{\pi}{25}\delta. \tag{5.9}$$

Then by an adaptation of a reasoning of BOHR one can deduce from our assumption (1.3) that for $n > c_7$ the inequality

$$\sum_{\nu \leqq n} \lambda(\nu)\nu^{-1-2\frac{\log^4 n}{\sqrt{n}}} \geqq 0 \tag{5.10}$$

holds. Using (5.3) this gives easily the inequality

$$L(x) \overset{\text{def}}{=} \sum_{\nu \leqq x} \frac{\lambda(\nu)}{\nu} > -c_{10}\frac{\log^4 x}{\sqrt{x}} > -x^{-\frac{1}{2}+\varepsilon} \tag{5.11}$$

for $x > c_{11}(\varepsilon)$, ε arbitrarily small positive. Since for $\sigma > 1$ the identity

$$\int_1^\infty \frac{L(x) + x^{-\frac{1}{2}+\varepsilon}}{x^s}\,dx = \frac{\zeta(2s)}{(s-1)\zeta(s)} + \frac{1}{s - \frac{1}{2} - \varepsilon} \tag{5.12}$$

holds, (5.11) gives owing to a theorem of LANDAU that the "outstanding" singularity of the right hand side of (5.12) is on the real axis. But this proves the theorem.

(Received April 26, 1960)

Remarks to the theory of semi-modular lattices

By G. SZÁSZ in Szeged

Dedicated to Professor L. Rédei on his 60th birthday

1. By a theorem of G. BIRKHOFF ([1], p. 105) a semi-modular lattice of finite length is complemented if and only if its greatest element is the join of atoms. The „only if" part of this theorem does not depend on the semi-modularity: it holds obviously for all atomic lattices too. The „if" part may be also considerably generalized: such a generalization is given in our Theorem 1.

In the first half of the proof of Theorem 1 we make use of semi-complements which are represented as joins of atoms. This fact makes one interested in semi-complements of this type. Here, considering a semi-modular lattice L, an arbitrary element e and a countable set P of atoms of L, we give in Theorem 2 a condition which is sufficient for the join of each finite subset of P to be a semi-complement of e.

Finally, using this Theorem, we generalize Theorem 2 of our earlier paper [6].

2. We begin with some definitions; for the concepts not mentioned in this section, see [1].

By an *upper-directed set* S we mean a partly ordered set having the following property: given $a, b \in S$, there exists some $c \in S$ satisfying $c \geqq a$ and $c \geqq b$.

A lattice L is called *upper-continuous* if: (i) L is complete; (ii) for each upper-directed subset $\{s_\delta\}_{\delta \in \Delta}$ and for each element t of L,

$$\left(\bigvee_{\delta \in \Delta} s_\delta\right) \cap t = \bigvee_{\delta \in \Delta} (s_\delta \cap t).$$

A lattice L will be called *semi-modular* if it satisfies the following condition due to S. MACLANE and R. CROISOT[1]): if a and b are incomparable

[1]) For lattices of finite length this condition is equivalent to that of [1], p. 100; see [2], p. 99, Théorème 4.

elements of L and x any element of L such that $a \cap b < x < a$, then there exists an element t such that $a \cap b < t \leqq b$ and $(x \cup t) \cap a = x$.

Further, if a lattice has a least or a greatest element, then we shall it denote by o and i, respectively.

Finally, for the definition of semi-complements, proper semi-complements and semi-complemented lattices, see [5].

3. In this section we shall make use of two lemmas.

Lemma 1. *Let L be an upper-continuous lattice, $\{p_\gamma\}_{\gamma \in \Gamma}$ a set of atoms and e an arbitrary element of L. If $e \cap \bigvee_{\gamma \in \Gamma_0} p_\gamma = o$ for each finite subset Γ_0 of Γ, then $e \cap \bigvee_{\gamma \in \Gamma} p_\gamma = o$ too.*

This is a corollary of Hilfssatz 1.7 of Chapter I of [3].

Lemma 2. *Let $p_1, \ldots, p_n$ be arbitrary atoms of a semi-modular lattice with least element o. Then the length of the interval $[o, p_1 \cup \cdots \cup p_n]$ is at most n.*

Proof. By Propriété 2 on page 90 of [2], all distinct elements of the set

$$o, p_1, p_1 \cup p_2, \ldots, p_1 \cup \cdots \cup p_n$$

form a maximal chain C between o and $p_1 \cup \cdots \cup p_n$. The length of C is at most n. Thus, Lemma 2 is implied by the Corollary of Theorem 1 in [4].

Now we prove

Theorem 1. *Let L be an upper-continuous semi-modular lattice with greatest element i. If there exists a set $\{p_\gamma\}_{\gamma \in \Gamma}$ of atoms in L such that $\bigvee_{\gamma \in \Gamma} p_\gamma = i$, then L is complemented and atomic*[2]).

Proof. In the first half of the proof we follow the way given in [3], pp. 78—79. Nevertheless, for the sake of completeness we give a full discussion.

Let a denote an arbitrary element of L different from o and i. Consider the family $\mathfrak{M}$ of all index sets $\Delta (\subseteq \Gamma)$ having the property

$$a \cap \bigvee_{\delta \in \Delta} p_\delta = o.$$

Then, firstly, $\mathfrak{M}$ is non-empty, because — by $a \neq i$ — $a \cap p_\gamma = o$ for some $\gamma \in \Gamma$. Next, let $\mathfrak{N}$ be a (non-empty) subchain of $\mathfrak{M}$ and $\Delta_{\mathfrak{N}}$ denote the (set-theoretical) union of all sets Δ belonging to $\mathfrak{N}$. We show $\Delta_{\mathfrak{N}} \in \mathfrak{M}$. Indeed, consider an arbitrary finite subset Δ of $\Delta_{\mathfrak{N}}$. Then, by the definition

[2]) For upper-continuous modular lattices, see [3], Chapter III, Satz 2.1.

of $\Delta_{\mathfrak{M}}$, there exists a set Δ' in $\mathfrak{M}$ which includes Δ. Consequently,

$$a \cap \bigvee_{\delta \in \Delta} p_\delta \leqq a \cap \bigvee_{\delta \in \Delta'} p_\delta = o.$$

Hence, by Lemma 1,

$$a \cap \bigvee_{\delta \in \Delta_{\mathfrak{M}}} p_\delta = o;$$

in other words, $\Delta_{\mathfrak{M}} \in \mathfrak{M}$.

By the preceding paragraph, the Zorn Lemma may be applied for $\mathfrak{M}$. It follows that there exists a maximal subset Δ^* of Γ, i. e. a maximal set Δ^* with the property

$$a \cap \bigvee_{\delta \in \Delta^*} p_\delta = o. \tag{1}$$

We show that just the element

$$b = \bigvee_{\delta \in \Delta^*} p_\delta \tag{2}$$

is a complement of a; by our assumption on $\{p_\gamma\}_{\gamma \in \Gamma}$, it suffice to prove that $a \cup b \geqq p_\gamma$ for all $\gamma \in \Gamma$. Clearly, $b \neq o$.

Suppose $p = p_{\gamma_0} \not\leqq a \cup b$ for some $\gamma_0 \in \Gamma$. Then $a \cup b$ and p are incomparable elements and

$$(a \cup b) \cap p = o. \tag{3}$$

On the other hand, $a \cup b \neq b$, because $a \cup b = b$ would imply, by (2) and (1), $o = a \cap b = a$, in contradiction to our assumption $a \neq o$. Hence

$$(a \cup b) \cap p < b < a \cup b.$$

It follows, by the semi-modularity of L, that there exists an element t such that

$$(a \cup b) \cap p < t \leqq p \tag{4}$$

and

$$(b \cup t) \cap (a \cup b) = b. \tag{5}$$

But, by (3) the inequalities (4) have no solution other than $t = p$. Therefore (5) implies

$$(b \cup p) \cap (a \cup b) = b.$$

From this equation we get, with respect to (2) and (1),

$$o = a \cap b = a \cap (a \cup b) \cap (b \cup p) = a \cap (b \cup p) =$$
$$= a \cap \Big(\bigvee_{\delta \in \Delta^*} p_\delta \cup p\Big) = a \cap \Big(\bigvee_{\delta \in \Delta^*} p_\delta \cup p_{\gamma_0}\Big),$$

which contradicts the maximality of Δ^*. Thus the first assertion of our theorem is proved.

Now we prove the second assertion. By definition,

$$a \cap \bigvee_{\gamma \in \Gamma} p_\gamma = a \cap i = a \neq o.$$

Therefore, by Lemma 1,

$$a \cap \bigvee_{\gamma \in \Gamma_0} p_\gamma \neq o$$

for some finite subset Γ_0 of Γ. Denote $c = \bigvee_{\gamma \in \Gamma_0} p_\gamma$. Then, by Lemma 2, the interval $[o, c]$ is of finite length. Consequently, there exists an atom q in $[o, c]$ such that $q \leqq a \cap c \leqq a$. This completes the proof of Theorem 1.

4. Now we deal with our above-mentioned theorems concerning semi-complements in semi-modular lattices.

Theorem 2. *Let e be an arbitrary element of a semi-modular lattice L with least element o. If the (finite or infinite) sequence $P = \{p_1, p_2, \ldots\}$ satisfies the condition*

$$(e \cup p_1 \cup \cdots \cup p_{k-1}) \cap p_k = o \qquad (k = 1, 2, \ldots), \tag{6}$$

then the join of every finite subset of P is a semi-complement of e.

Proof. Denote

$$e \cap (p_1 \cup \cdots \cup p_r) = d_r \qquad (r = 1, 2, \ldots). \tag{7}$$

Clearly, it suffices to show $d_r = o$ for each r.

Let us consider a d_r with fixed r. Since by (7) $e \geqq d_r$, we have

$$(e \cup p_1 \cup \cdots \cup p_{k-1}) \cap p_k \geqq (d_r \cup p_1 \cup \cdots \cup p_{k-1}) \cap p_k$$

for $k = 1, \ldots, r$. Hence, by our assumption (6),

$$p_k \not\leqq d_r \cup p_1 \cup \cdots \cup p_{k-1} \qquad (k = 1, \ldots, r).$$

This implies, together with (7),

$$d_r < d_r \cup p_1 < \cdots < d_r \cup p_1 \cup \cdots \cup p_r = p_1 \cup \cdots \cup p_r. \tag{8}$$

On the other hand, by Lemma 2, the length of the interval $[o, p_1 \cup \cdots \cup p_r]$ does not exceed r. Thus from (8) we conclude $d_r = o$.

As a corollary of Theorem 2 we get

Theorem 3. *Let L be a semi-complemented semi-modular atomic lattice. If an element $e (\neq o)$ of L has no complement, then to each non-negative integer ν there exists a semi-complement of e whose height is equal to ν.*

Proof. Being L semi-complemented, e has a proper semi-complement x_1. Since L is atomic too, there exists an atom p_1 in L such that $p_1 \leqq x_1$. Then $e \cap p_1 \leqq e \cap x_1 = o$. If e has no complement, then $e \cup p_1$ ($\neq i$ and thus it)

has also a proper semi-complement x_2. Again, there exists an atom p_2 such that $p_2 \leqq x_2$ and $(e \cup p_1) \cap p_2 = o$; and so on. Applying now Theorem 2, we get Theorem 3.

References

[1] G. Birkhoff, *Lattice theory*, revised edition (New York, 1948).

[2] M. L. Dubreil-Jacotin—L. Lesieur—R. Croisot, *Leçons sur la théorie des structures algébriques ordonnées et des treillis géométriques*, Cahiers scientifiques **21**, Gauthier-Villars (Paris, 1953).

[3] F. Maeda, *Kontinuierliche Geometrien* (Berlin—Göttingen—Heidelberg, 1958).

[4] G. Szász, On the structure of semi-modular lattices of infinite length, *Acta Sci. Math.*, **14** (1952), 239—245.

[5] ———, On weakly complemented lattices, *Acta Sci. Math.*, **16** (1955), 122—126.

[6] ———, Semi-complements and complements in semi-modular lattices, *Publicationes Math. Debrecen*, **5** (1957-58), 217—221.

(Received April 26, 1960)

Der Normalisator einer subnormalen Untergruppe

Von HELMUT WIELANDT in Tübingen (Deutschland)

Ladislaus Rédei zum 60. Geburtstag am 15. November 1960

§ 1. Übersicht

G sei eine endliche Gruppe; A sei eine subnormale Untergruppe von G, also erreichbar durch eine mit G beginnende absteigende Normalkette. Man weiß dann, daß der Normalisator $\mathfrak{N}A$ von A in G „groß" ist. Es versteht sich von selbst, daß aus $A \neq G$ auch $A \neq \mathfrak{N}A$ folgt. Darüber hinaus kennt man verschiedene Aussagen über die Größe von $\mathfrak{N}A$; sie sind in § 2 zusammengestellt.

Die folgende Untersuchung bewegt sich in der gleichen Richtung, aber unter Verwendung eines neuen Hilfsmittels: sie berücksichtigt den Anteil der einzelnen Primzahlen an A. Diesen kann man auf zwei Arten erklären. Man kann zu jeder Primzahl p entweder eine p-Sylowgruppe A_p wählen, oder man kann des Erzeugnis pA aller p-Sylowgruppen von A bilden. Zwischen den Normalisatoren $\mathfrak{N}pA$ und $\mathfrak{N}A$ ergibt sich ein einfacher Zusammenhang (3. 5. 1), nämlich $\mathfrak{N}A = \cap \mathfrak{N}pA$. Daher beschäftigen wir uns eingehend mit $\mathfrak{N}pA$. Dieser Normalisator hängt eng mit $\mathfrak{N}A_p$ zusammen; die in einer früheren Arbeit [4] entwickelte Methode der Projektion von A in eine p-Sylowgruppe von G gibt genaue Aufschlüsse. Das Hauptgewicht liegt auf der Frage, wann pA eine normale oder sogar charakteristische Untergruppe von G oder von pG ist. Ein einfaches Ergebnis sei als Beispiel genannt:

Satz 1.1. *Sei A subnormal in G, und sei A_p eine p-Sylowgruppe von A.*

(a) *Genau dann ist pA normal in pG, wenn A_p normal ist in allen denjenigen p-Sylowgruppen von G, welche A_p enthalten.*

(b) *Genau dann ist pA eine charakteristische Untergruppe von G, wenn für jede Gruppe Γ von Automorphismen von G, für welche das Erzeugnis A_p^Γ der Bilder von A_p eine p-Gruppe ist, $A_p^\Gamma = A_p$ gilt.*

Die Voraussetzung von (a) ist zum Beispiel dann erfüllt, wenn eine p-Sylowgruppe von G abelsch ist; und die Voraussetzung von (b) dann, wenn A_p in jeder größeren p-Untergruppe von G charakteristisch ist.

Das Hauptergebnis dieser Note ist ein erheblich schärferer Satz (5. 3); er ist zugleich insofern allgemeiner, als in ihm π-Hallgruppen anstelle der p-Sylowgruppen betrachtet werden.

Bezeichnungen. $A, B, \ldots$ sind Untergruppen einer endlichen Gruppe G. Erzeugnis und Durchschnitt bezeichnen wir mit $\cup$ und $\cap$, das neutrale Element von G mit 1. Wir schreiben $b^{-1}Ab = A^b$ und $\bigcup_{b \in B} A^b = A^B$.

Mit $\mathbf{n}A, \mathbf{s}A, \mathbf{u}A$ bezeichnen wir der Reihe nach die Menge der normalen, subnormalen, aller Untergruppen von A. Für jede Teilmenge $\mathbf{m} \subseteq \mathbf{u}A$ bezeichne $\mathbf{N}\mathbf{m}$ den Durchschnitt der (in G zu bildenden) Normalisatoren $\mathbf{N}M$ ($M \in \mathbf{m}$). Unter der normalen Hülle von A in G verstehen wir die Gruppe $A^G = \bigcap N$ ($A \subseteq N \in \mathbf{n}G$); die subnormale Hülle von A in G bezeichnen wir mit $A^{\cdot G}$; sie ist durch $A^{\cdot G} = \bigcap S$ ($A \subseteq S \in \mathbf{s}G$) erklärt.

Mit p, q bezeichnen wir stets Primzahlen, mit π, ϱ Mengen von Primzahlen. Für jede natürliche Zahl n verstehen wir unter n_π den Anteil von π an n: es ist $n_\pi = \Pi' p^\alpha$ ($p \in \pi$), wenn Πp^α die Primfaktorzerlegung von n ist. Die Ordnung von A bezeichnen wir mit $|A|$, den Index von A in G mit $|G:A|$. Wie üblich, heißt A eine π-Gruppe, wenn $|A| = |A|_\pi$ ist; und A heißt eine π-Hallgruppe von G, wenn $|A| = |G|_\pi$ ist. Die p-Hallgruppen sind die p-Sylowgruppen. Das Erzeugnis aller π-Untergruppen von A bezeichnen wir ständig mit πA.

§ 2. Bekannte Ergebnisse

Über den Normalisator einer subnormalen Untergruppe sind bisher im wesentlichen drei Sätze bekannt.

2. 1. *Seien $A, B \in \mathbf{s}G$; B enthalte A nicht; A enthalte nur einen einzigen maximalen Normalteiler M, und die Faktorgruppe A/M sei nicht abelsch. Dann ist $B \subseteq \mathbf{N}A$* [3, Satz 20].

2. 2. *Seien $A, B \in \mathbf{s}G$; für keinen maximalen Normalteiler von A sei die Faktorgruppe isomorph zu einer der Kompositionsfaktorgruppen von B bis $A \cap B$ (in irgendeiner durch $A \cap B$ gelegten Kompositionsreihe von B). Dann ist $B \subseteq \mathbf{N}A$* [3, Satz 25].

2. 3. *Sei A subnormal in G; sei B entweder ein minimaler Normalteiler von G oder eine einfache, nicht abelsche, subnormale Untergruppe von G. Dann ist $B \subseteq \mathbf{N}A$* [5, Satz 1].

Außer diesen Ergebnissen werden wir die folgenden bekannten Tatsachen über subnormale Untergruppen und Hallgruppen benutzen.

2. 4. *Seien* $A, B \in \mathbf{s}G$. *Dann ist* $A \cup B \in \mathbf{s}G$ *und* $A \cap B \in \mathbf{s}G$. *Jede Kompositionsfaktorgruppe zwischen* $A \cup B$ *und* B *ist zu einer Kompositionsfaktorgruppe zwischen* A *und* $A \cap B$ *isomorph; daher ist jede Kompositionsfaktorgruppe von* $A \cup B$ *zu einer von* A *oder* B *isomorph* [3, Sätze 4, 7, 9].

2. 5. $(\pi \cup \varrho)A = \pi A \cup \varrho A$, *wenn* $A \in \mathbf{u}G$ [4, Satz 1. 2].

2. 6. $\pi(A \cup B) = \pi A \cup \pi B$, *wenn* $A, B \in \mathbf{s}G$ [4, Satz 1. 3].

2. 7. *Sei* $A \in \mathbf{s}G$ *und* G_π *eine* π*-Hallgruppe von* G. *Dann ist der Durchschnitt* $A_\pi = A \cap G_\pi$ *eine* π*-Hallgruppe von* A. *Wenn außerdem* $B \in \mathbf{s}G$ *ist, so gilt* $(A \cap B)_\pi = A_\pi \cap B_\pi$ *und* $(A \cup B)_\pi = A_\pi \cup B_\pi$ [6, Satz 2. 5].

§ 3. Zusammenhänge zwischen $\mathbf{N}A$ und $\mathbf{N}\pi A$

Wie stets sei π eine Menge von Primzahlen, πA das Erzeugnis aller π-Untergruppen von A. Bevor wir die Normalisatoren $\mathbf{N}A$ und $\mathbf{N}\pi A$ in Verbindung bringen, schicken wir drei Bemerkungen voraus.

3. 1. πA *ist der Durchschnitt derjenigen* $B \in \mathbf{s}A$, *für welche der Index* $|A:B|$ *keinen Primteiler aus* π *enthält.*

Beweis. Ist $B \in \mathbf{u}A$ und $|A:B|$ durch keine Primzahl aus π teilbar, so enthält B zu jedem $p \in \pi$ eine p-Sylowgruppe von A. Ist überdies $B \in \mathbf{s}A$, so enthält B sogar alle p-Sylowgruppen von A; das folgt für $B \in \mathbf{n}A$ aus der Konjugiertheit der Sylowgruppen und dann für $B \in \mathbf{s}A$ durch Induktion. Die in 3. 1 genannten Gruppen B sind also diejenigen Subnormalteiler von A, welche für jedes $p \in \pi$ alle p-Sylowgruppen von A enhalten. Ihr Durchschnitt D hat dann die gleiche Eigenschaft, daher ist $\pi A \subseteq D$. Daß umgekehrt $D \subseteq \pi A$ ist, versteht sich von selbst; denn πA ist eine der betrachteten Gruppen B.

3. 2. *Genau dann ist* $\pi A = A$, *wenn der Index jedes maximalen Normalteilers von* A *einen Primfaktor aus* π *enthält.*

Beweis. Ist $\pi A = A$, so ist nach 3. 1 der Index jedes maximalen Normalteilers von A durch eine Primzahl aus π teilbar. Ist umgekehrt diese Bedingung erfüllt, so gilt sie für jeden echten Normalteiler von A, aber nicht für πA. Daher ist $\pi A = A$.

3. 3. *Sei* $A \in \mathbf{s}G$ *und* $b \in B \subseteq G$. *Dann gilt* $\pi(A^b) = (\pi A)^b$ *und* $\pi(A^B) = (\pi A)^B$.

Man darf also kurz πA^b und πA^B schreiben.

Beweis: Die erste Aussage folgt aus der Tatsache, daß die Abbildung $a \to a^b$ ein Isomorphismus ist; die zweite ergibt sich durch wiederholte Anwendung von 2. 6.

Wir untersuchen nun die Zusammenhänge zwischen den Normalisatoren $\mathbf{N}\pi_i A$ für beliebige Mengen π_i von Primzahlen.

3. 4. *Sei* $A \in \mathbf{u}G$. *Dann ist* $\mathbf{N} \cup \pi_i A = \cap \mathbf{N}\pi_i A$.

Beweis. Es ist offenbar $\pi_j A = \pi_j(\cup \pi_i A)$. Daher ist $\pi_j A$ eine charakteristische Untergruppe von $\cup \pi_i A$. Also gilt in der Behauptung von 3. 4 das Zeichen $\subseteq$. Da andererseits die $\pi_i A$ die Gruppe $\cup \pi_i A$ erzeugen, gilt auch das Zeichen $\supseteq$.

Nach 3. 4 kann $\mathbf{N}A$ bestimmt werden, wenn man $\mathbf{N}\pi_i A$ für hinreichend große π_i kennt. Was unter „hinreichend groß" zu verstehen ist, ergibt sich mittels 2. 5 und 3. 2:

Satz 3. 5. *Es seien* $\pi_1, \pi_2, \ldots$ *Primzahlmengen derart, daß der Index jedes maximalen Normalteilers von* A *mindestens einen Primfaktor aus* $\cup \pi_i$ *enthält. Dann ist* $\mathbf{N}A = \cap \mathbf{N}\pi_i A$.

Die Voraussetzung ist sicher dann erfüllt, wenn $\cup \pi_i$ alle Primteiler von $|A|$ enthält. Daher gilt

3. 5. 1. *Es ist* $\mathbf{N}A = \cap \mathbf{N}pA$, *wenn* p *alle Primteiler von* $|A|$ *durchläuft.*

Teilaussagen über $\mathbf{N}A$ kann man mitunter schon aus Kenntnis eines Normalisators $\mathbf{N}\pi A$ gewinnen; so kann man 2. 2 verallgemeinern:

Satz 3. 6. *Sei* $A \in \mathbf{s}G$, $B \in \mathbf{u}G$. *Es sei entweder* $B \in \mathbf{s}G$ *oder* $AB = BA$. *Sei* $B \subseteq \mathbf{N}\pi A$. *Für keinen maximalen Normalteiler* M *von* A *mit* $|A : M|_\pi = 1$ *sei* A/M *isomorph zu einer der Kompositionsfaktorgruppen von* B *bis* $A \cap B$. *Dann ist* $B \subseteq \mathbf{N}A$.

Beweis. Indem wir von G zu $A \cup B$ übergehen, können wir annehmen, daß πA in G normal ist; und indem wir zur Faktorgruppe nach πA übergehen, können wir auch $\pi A = 1$ annehmen. Dann ist keine einfache Faktorgruppe von A zu einer der Kompositionsfaktorgruppen F von B bis $A \cap B$ isomorph. Aber jede Kompositionsfaktorgruppe von G bis A ist zu einer solchen Gruppe F isomorph, denn sie stimmt mit einer Kompositionsfaktorgruppe zwischen B und $A \cap B$ überein (das ist, wenn $B \in \mathbf{s}G$, eine Teilaussage von 2. 4; im Fall $AB = BA = G$ ist es leicht unmittelbar einzusehen). Also jede einfache Faktorgruppe von A ist verschieden von jeder Kompositionsfaktorgruppe zwischen G und A. Hieraus folgt nach 2. 4 leicht, daß A in G charakteristisch ist; insbesondere ist $B \subseteq \mathbf{N}A$, wie behauptet.

Die beiden letzten Sätze führen die Untersuchung von $\mathbf{N}A$ für subnormale A auf die Untersuchung geeigneter Normalisatoren $\mathbf{N}\pi A$ zurück.

§ 4. Der Normalisator von πA

Seien $A \in \mathfrak{s}G$ und eine Primzahlmenge π gegeben. Wir suchen Bedingungen, unter denen $\mathbf{N}\pi A$ groß ist. Ein erstes Ergebnis können wir durch die eben benutzte Schlußweise erhalten:

Satz 4.1. *Sei $A \in \mathfrak{s}G$, $B \in \mathfrak{u}G$. Es sei entweder $B \in \mathfrak{s}G$ oder $AB = BA$. Der Index $|B : A \cap B|$ enthalte keinen Primteiler aus π. Dann ist πA eine charakteristische Untergruppe von $A \cup B$, nämlich $\pi A = \pi(A \cup B)$; insbesondere ist $B \subseteq \mathbf{N}\pi A$.*

Beweis: Jeder Kompositionsfaktor zwischen $A \cup B$ und A ist, wie der Beweis von 3.6 gezeigt hat, auch ein Kompositionsfaktor zwischen B und $A \cap B$. Also enthält $|A \cup B : A|$ keinen Primteiler aus π. Daher enthält auch $|A \cup B : \pi A|$ keinen Primteiler aus π. Da $\pi A \in \mathfrak{s}(A \cup B)$ ist, zeigt 3.1, daß $\pi(A \cup B) \subseteq \pi A$ ist. Die umgekehrte Beziehung ist trivial.

Verwandte Ergebnisse unter schwächeren Voraussetzungen können wir mit Hilfe der „Projektion von $\mathfrak{s}G$ in Hallgruppen" erhalten, die durch 2.7 beschrieben wird. Hierfür müssen wir die Existenz einer π-Hallgruppe in G voraussetzen. Das bedeutet für die Anwendung keine starke Einschränkung; denn es kommt vor allem der Fall in Betracht, daß π aus einer einzigen Primzahl besteht, und dann ist die Existenz der Hallgruppe durch den Satz von SYLOW gesichert.

Ständige Voraussetzung. In diesem Abschnitt bezeichnen wir mit G_π stets eine fest gewählte π-Hallgruppe von G; für jedes $A \in \mathfrak{s}G$ setzen wir $A_\pi = A \cap G_\pi$.

Nach 2.7 ist A_π eine π-Hallgruppe von A. Zwischen A_π und πA besteht ein enger Zusammenhang:

4.2. *Es ist $\pi A = A_\pi^{\cdot\cdot A} = A_\pi^{\cdot\cdot G}$ und $A_\pi = \pi A \cap G_\pi$.*

Beweis. Da $|A : A_\pi|$ keinen Primteiler aus π enthält, gilt das Gleiche für $|A : A_\pi^{\cdot\cdot A}|$. Daher ist $\pi A \subseteq A_\pi^{\cdot\cdot A}$. Andererseits haben wir $A_\pi \subseteq \pi A \in \mathfrak{s}A$ nach Definition von πA; also ist auch $\pi A \supseteq A_\pi^{\cdot\cdot A}$. Ferner ist $A_\pi^{\cdot\cdot A} = A_\pi^{\cdot\cdot G}$; denn wegen $A_\pi \subseteq A_\pi^{\cdot\cdot G} \in \mathfrak{s}G$ haben wir $A_\pi^{\cdot\cdot A} \subseteq A_\pi^{\cdot\cdot G}$, und andererseits ist wegen $\mathfrak{s}A \subseteq \mathfrak{s}G$ natürlich $A_\pi^{\cdot\cdot G} \subseteq A_\pi^{\cdot\cdot A}$. Damit ist die erste Behauptung bewiesen; die zweite folgt unmittelbar aus der Definition von A_π und πA.

Wir können nun einen Zusammenhang zwischen $\mathbf{N}A_\pi$ und $\mathbf{N}\pi A$ herstellen:

Satz 4.3. *Es ist $\mathbf{N}A_\pi \subseteq \mathbf{N}\pi A$.*

Beweis. Die von $\mathbf{N}A_\pi$ induzierten inneren Automorphismen von G lassen A_π fest. Sie lassen daher auch die subnormale Hülle $A_\pi^{\cdot\cdot G}$ fest; diese stimmt nach 4.2 mit πA überein.

Man kann 4.3 so aussprechen: Aus $B \subseteq \mathbf{N}A_\pi$ folgt $B \subseteq \mathbf{N}\pi A$. Hieraus kann man eine nützliche hinreichende Bedingung dafür gewinnen, daß die normale Hülle $B^G \subseteq \mathbf{N}\pi A$ ist:

Satz 4.4. *Sei $A \in \mathbf{s}G$, $B \in \mathbf{u}G$. Für jedes $g \in G$ gelte $B \subseteq \mathbf{N}(A^g \cap G_\pi)$. Dann ist $B^G \subseteq \mathbf{N}\pi A$.*

Beweis. Für jedes $g \in G$ ist nach Voraussetzung $B^g \subseteq \mathbf{N}(A \cap G_\pi^g)$. Wendet man den vorigen Satz auf G_π^g anstelle von G_π an, so ergibt sich $B^g \subseteq \mathbf{N}\pi A$ für alle $g \in B$. Also ist $B^G \subseteq \mathbf{N}\pi A$.

Wir geben einige Beispiele für die Anwendung des Satzes 4.4; dabei ist, wie stets in diesem Abschnitt, $A \in \mathbf{s}G$ vorausgesetzt.

4.4.1. *Es ist $\mathbf{N}\mathbf{s}G_\pi \subseteq \mathbf{N}\pi A$, wenn $\mathbf{N}\mathbf{s}G_\pi = \bigcap \mathbf{N}S$ $(S \in \mathbf{s}G_\pi)$ gesetzt wird.*

So gehört zum Beispiel das Zentrum jeder π-Hallgruppe von G zu $\mathbf{N}\pi A$. Wir heben den Fall $\pi = p$ hervor:

4.4.2. *Das Zentrum jeder p-Sylowgruppe von G liegt in $\mathbf{N}pA$.*

Tiefere Hilfsmittel benutzt die folgende Anwendung von 4.4:

4.4.3. *Sei $A \in \mathbf{s}G$. Die p-Sylowgruppen von G seien regulär im Sinn von* Hall [1] *(hierfür genügt z. B., daß ihre Klasse kleiner als p ist). Die Ordnungen aller Elemente der p-Sylowgruppen von A mögen eine bestimmte Potenz p^α teilen, und es sei b ein Element von G, dessen Ordnung eine Potenz von p ist und das sich als p^α-te Potenz eines Elements von G darstellen läßt. Sei B die von b erzeugte zyklische Gruppe und B^G ihre normale Hülle. Dann ist $B^G \subseteq \mathbf{N}pA$.*

Beweis. Wir wählen eine p-Sylowgruppe G_p von G, die eine p^α-te Wurzel aus b enthält. In einer regulären p-Gruppe ist jede p^α-te Potenz mit jedem Element vertauschbar, dessen Ordnung p^α teilt [1, Th. 4.461]. Also ist $B \subseteq \mathbf{N}(A^g \cap G_p)$ für jedes $g \in G$. Nach 4.4 ist $B^G \subseteq \mathbf{N}pA$.

Eine andere Folgerung bezieht sich auf zwei Primzahlmengen π, ϱ:

Satz 4.5. *Der Index $|G : \bigcap_{g \in G} \mathbf{N}(A^g \cap G_\pi)|$ sei durch keine Primzahl aus ϱ teilbar. Dann ist $\varrho G \subseteq \mathbf{N}\pi A$.*

Beweis. Sei $q \in \varrho$. Dann enthält $\bigcap \mathbf{N}(A^g \cap G_\pi)$ eine q-Sylowgruppe B von G. Diese erfüllt die Voraussetzungen von Satz 4.4, also ist $B^G \subseteq \mathbf{N}\pi A$. Nach Sylow ist $B^G = qG$. Also enthält $\mathbf{N}\pi A$ das Erzeugnis aller Gruppen $qG, q \in \varrho$; es stimmt nach 2.5 mit ϱG überein.

Wir heben einen einfachen Sonderfall hervor:

4.5.1. *G enthalte eine π-Hallgruppe G_π und eine ϱ-Hallgruppe G_ϱ, die elementweise vertauschbar sind. Dann ist $\varrho G \subseteq \mathbf{N}\pi A$ für jedes $A \in \mathbf{s}G$.*

Nach 4.4.1 würde sogar schon die schwächere Voraussetzung $G_\varrho \subseteq \mathbf{N}_\mathbf{s} G_\pi$ genügen.

Von nun an setzen wir statt $B \in \mathbf{u}G$ schärfer $B \in \mathbf{s}G$ voraus; dann ist $B_\pi = B \cap G_\pi$ erklärt. Wir untersuchen die Frage, wann $\pi B \subseteq \mathbf{N}\pi A$ ist. Notwendig hierfür ist $B_\pi \subseteq \mathbf{N}A_\pi$, weil $B_\pi = \pi B \cap G_\pi$ und $A_\pi = \pi A \cap G_\pi$ ist (4.2). Man könnte vermuten, daß aus $B_\pi \subseteq \mathbf{N}A_\pi$ umgekehrt auch $\pi B \subseteq \mathbf{N}\pi A$ folgt. Doch wird diese Vermutung durch das folgende Gegenbeispiel widerlegt; es zeigt sogar noch etwas mehr, nämlich daß aus $G_p \subseteq \mathbf{N}A_p$ nicht notwendig $pG \subseteq \mathbf{N}pA$ folgt.

Beispiel 4.6. Sei C die Permutationsgruppe des Grades 6, die durch die drei Transpositionen (1 2), (3 4), (5 6) erzeugt wird. Sei G der Normalisator von C in der symmetrischen Gruppe des Grades 6; G ist eine transitive Gruppe der Ordnung 48. Sei A die von (1 2) erzeugte Gruppe der Ordnung 2 und G_2 die von C zusammen mit (3 5)(4 6) erzeugte Gruppe der Ordnung 16. Dann ist G_2 eine 2-Sylowgruppe von G, es ist $A \in \mathbf{s}G$, ferner ist $A \cap G_2$ normal in G_2, aber die Gruppe $2A = A$ ist nicht normal in der Gruppe $2G = G$.

Um auf $\pi B \subseteq \mathbf{N}\pi A$ zu schließen, braucht man also stärkere Voraussetzungen als $B_\pi \subseteq \mathbf{N}A_\pi$. Wir geben eine notwendige und hinreichende Bedingung an:

Satz 4.7. *Seien $A, B \in \mathbf{s}G$. Genau dann ist $\pi B \subseteq \mathbf{N}\pi A$, wenn $B \cap G_\pi \subseteq \mathbf{N}(A^b \cap G_\pi)$ gilt für jedes $b \in \pi B$.*

Beweis. (a) Sei $\pi B \subseteq \mathbf{N}\pi A$. Dann haben wir $\pi B \subseteq \mathbf{N}\pi A^b$ für jedes $b \in \pi B$; schneiden wir mit G_π, so erhalten wir $\pi B \cap G_\pi \subseteq \mathbf{N}(\pi A^b \cap G_\pi)$. Es ist $\pi B \cap G_\pi = B \cap G_\pi$, entsprechend für A^b, also ist $B \cap G_\pi \subseteq \mathbf{N}(A^b \cap G_\pi)$.

(b) Ist die letzte Beziehung erfüllt, so haben wir für jedes $b \in \pi B$, wie 4.3 zeigt, $\pi B \cap G_\pi \subseteq \mathbf{N}\pi A^b$, also $(\pi B \cap G_\pi)^{b^{-1}} \subseteq \mathbf{N}\pi A$. Die auf der linken Seite stehenden Gruppen erzeugen, wenn wir b alle Elemente von πB durchlaufen lassen, die normale Hülle der π-Hallgruppe $\pi B \cap G_\pi$ in πB, das ist aber πB selbst (3.1). Folglich ist $\pi B \subseteq \mathbf{N}\pi A$, wie behauptet.

Wir behandeln die entsprechende Frage für πB^G statt πB:

Satz 4.8. *Seien $A, B \in \mathbf{s}G$. Genau dann ist $\pi B^G \subseteq \mathbf{N}\pi A$, wenn $B \cap G_\pi \subseteq \mathbf{N}(A^g \cap G_\pi)$ gilt für alle $g \in G$.*

Beweis. Jede der nachstehenden Aussagen ist, wie man mit Hilfe von 4.7 sieht, der folgenden gleichwertig; dabei sollen g, b alle Elemente von $G, \pi B$ durchlaufen.

$$\pi B^g \subseteq \mathbf{N}\pi A,\ \pi B \subseteq \mathbf{N}\pi A^g,\ B \cap G_\pi \subseteq \mathbf{N}(A^{gb} \cap G_\pi),\ B \cap G_\pi \subseteq \mathbf{N}(A^g \cap G_\pi).$$

Wir heben den Sonderfall $B = G$ hervor:

4. 8. 1. *Genau dann ist* $\pi G \subseteq \mathbf{N}\pi A$, *wenn* $G_\pi \subseteq \mathbf{N}(A^g \cap G_\pi)$ *ist für jedes* $g \in G$.

Wir können diese Bedingung für alle $A \in \mathbf{s}G$ gleichzeitig formulieren, indem wir mit $\mathbf{s}_G G_\pi$ den Verband aller Durchschnitte $A \cap G_\pi$ bezeichnen ($A \in \mathbf{s}G$). Wir erhalten

4. 8. 2. *Genau dann ist* $\pi G \subseteq \mathbf{N}\pi A$ *für alle* $A \in \mathbf{s}G$, *wenn* $\mathbf{s}_G G_\pi \subseteq \mathbf{n} G_\pi$ *ist.*

Zum Schluß dieses Abschnitts geben wir eine hinreichende Bedingung dafür an, daß πA in G charakteristisch ist:

Satz 4. 9. *Sei* $A \in \mathbf{s}G$. *Keine subnormale Untergruppe von* G_π *habe die Ordnung* $|A \cap G_\pi|$, *außer* $A \cap G_\pi$ *selbst. Dann ist* πA *eine charakteristische Untergruppe von* G. *Genauer gilt: Ist* $B \in \mathbf{s}G$ *und* $|\pi B|_\pi = |\pi A|_\pi$, *so ist* $\pi B = \pi A$.

Beweis. Es ist $|B \cap G_\pi| = |\pi B|_\pi = |A \cap G_\pi|$, also ist nach Voraussetzung $B \cap G_\pi = A \cap G_\pi$. Hieraus folgt nach 4. 2 $\pi B = \pi A$.

§ 5. Verschärfung unter Konjugiertheitsvoraussetzungen für Hallgruppen

Die Sätze des vorigen Abschnitts lassen sich in dem Fall, daß π nur aus einer einzigen Primzahl besteht, verschärfen. Das beruht auf dem Satz von SYLOW, nach dem je zwei p-Sylowgruppen konjugiert sind. Das Entsprechende für π-Hallgruppen gilt nicht allgemein. Wir können die erwähnten Verschärfungen aber trotzdem allgemein formulieren, indem wir die benötigten Konjugiertheitsvoraussetzungen von Fall zu Fall aussprechen. Die Existenz einer π-Hallgruppe von G setzen wir nur dort voraus, wo es ausdrücklich erwähnt ist.

Wir beginnen damit, die früher bewiesene Beziehung $\mathbf{N}A_\pi \subseteq \mathbf{N}\pi A$ zu einer Gleichung zu verschärfen:

5. 1. *Sei* $A \in \mathbf{s}G$. A *enthalte eine* π*-Hallgruppe* A_π *mit der Eigenschaft, daß zu jedem* $g \in \mathbf{N}\pi A$ *ein* $a \in \pi A$ *existiert, für das* $A_\pi^g = A_\pi^a$ *ist. Dann ist* $\mathbf{N}\pi A = \pi A \cdot \mathbf{N}A_\pi = \mathbf{N}A_\pi \cdot \pi A$.

Beweis. Nach 4. 3 ist $\mathbf{N}A_\pi \subseteq \mathbf{N}\pi A$, daher ist πA mit $\mathbf{N}A_\pi$ vertauschbar. Die beiden letzten Ausdrücke in 5. 1 stimmen also überein, und es ist $\mathbf{N}A_\pi \cdot \pi A \subseteq \mathbf{N}\pi A$.

Es ist noch zu zeigen, daß jedes $g \in \mathbf{N}\pi A$ in der Form $g = ha$ mit $h \in \mathbf{N}A_\pi$, $a \in \pi A$ dargestellt werden kann. Zu diesem Zweck wählen wir $a \in \pi A$ derart, daß $A_\pi^g = A_\pi^a$ ist, und setzen $h = ga^{-1}$. Dann wird, wie gewünscht, $g = ha$ und $A_\pi^h = A_\pi$.

Es muß betont werden, daß die Konjugiertheitsvoraussetzung von 5.1 keineswegs immer erfüllt ist, selbst wenn A eine π-Hallgruppe A_π enthält. Zum Beispiel gibt es in der einfachen Gruppe G_{168} zwei nicht konjugierte Halluntergruppen der Ordnung 24, die durch einen Automorphismus der Ordnung 2 von G_{168} ineinander übergeführt werden können. Es erhebt sich daher die Frage nach Bedingungen, welche für die Existenz einer π-Hallgruppe mit der verlangten Eigenschaft hinreichen. Auf diese Frage gehen wir später ein (5.4, 5.5).

Wir heben den Sonderfall von 5.1 hervor, in dem π nur eine einzige Primzahl enthält:

5.1.1. *Sei $A \in \mathfrak{s}G$, und A_p sei eine p-Sylowgruppe von A. Dann ist* $\mathbf{N}pA = pA \cdot \mathbf{N}A_p = \mathbf{N}A_p \cdot pA$.

Das wesentliche Hilfsmittel der weiteren Untersuchung ist der folgende auch für unendliche Gruppen G gültige Hilfssatz:

5.2. *Sei $A \in \mathfrak{s}G$ und $A^G \cdot \mathbf{N}A = G$. Dann ist A normal in G.*

Beweis. Wir bilden die absteigende Reihe der normalen Hüllen von A, also die Gruppen $G_0 = G$, $G_1 = A^{G_0}$, $G_2 = A^{G_1}$ usw. Wegen der Subnormalität von A bricht diese Reihe nach endlich vielen, etwa r, Schritten mit $G_r = A$ ab. Nach unseren Voraussetzungen ist $G_1 = A^G = A^{\mathbf{N}A \cdot G_1} = A^{G_1} = G_2$, also ist $r = 1$, daher ist A normal in G.

Durch eine geringe Änderung des Beweises läßt sich, wie im Vorbeigehen erwähnt werden soll, 5.2 folgendermaßen verschärfen:

5.2.1. *Sei $A \in \mathfrak{s}G$. Sei $G = G_0 \supset G_1 \supset \cdots \supset G_r = A$ irgendeine von G nach A führende Normalkette kürzester Länge. Sei $G_1\mathbf{N}A = G$. Dann ist $r = 1$, also A normal in G.*

Nach diesen Vorbereitungen können wir eine Reihe notwendiger und hinreichender Bedingungen für Normalität von πA in G beweisen. Wir fassen sie zusammen zum

Hauptsatz 5.3. *Sei $A \in \mathfrak{s}G$. In dem Normalteiler $H = \pi A^G$ von G existiere eine π-Hallgruppe H_π mit der folgenden Eigenschaft: (*) Zu jedem $g \in G$ gibt es ein $h \in H$, für das $H_\pi^g = H_\pi^h$ ist.*

Wir setzen $A \cap H_\pi = A_\pi$. Dann sind je zwei der folgenden Aussagen gleichwertig:

(a) πA *ist normal in* G.

(b) *Wenn* U *eine Untergruppe von* G *derart ist, daß* A_π^U *eine* π*-Gruppe ist, so ist stets* $A_\pi^U = A_\pi$.

(c) *Es ist* $\mathbf{N}H_\pi \subseteqq \mathbf{N}A_\pi$.

(d) *Es gibt eine Gruppe* $U \subseteqq \mathbf{N}H_\pi$ *derart, daß* $HU^G = G$ *ist und daß aus* $g \in G$ *und* $U^g \subseteq \mathbf{N}H_\pi$ *stets* $U^g \subseteqq \mathbf{N}A_\pi$ *folgt.*

Verfahren zur Konstruktion einer Gruppe H_π mit den benötigten Eigenschaften werden unter geeigneten Voraussetzungen in 5.4 und 5.5 angegeben.

Beweis. *Aus* (a) *folgt* (b). Sei πA normal in G, $U \in \mathbf{u}G$, A_π^U eine π-Gruppe. Dann ist $\pi A \cap A_\pi^U$ eine π-Untergruppe von A, welche die π-Hallgruppe A_π enthält; daher ist $\pi A \cap A_\pi^U = A_\pi$. Wegen $U \subseteqq \mathbf{N}\pi A \cap \mathbf{N}A_\pi^U$ ist $U \subseteqq \mathbf{N}A_\pi$, wie behauptet.

Aus (b) *folgt* (c). Man kann in (b) $U = \mathbf{N}H_\pi$ wählen.

Aus (c) *folgt* (d). Wir wählen $U = \mathbf{N}H_\pi$; dann ist $HU^G \supseteqq HU = H\mathbf{N}H_\pi$, und nach 5.1, auf $H = \pi H$ statt A angewendet, stimmt $H\mathbf{N}H_\pi$ mit $\mathbf{N}H = G$ überein. Also ist $HU^G = G$, wie behauptet. Aus $g \in G$ und $U^g \subseteqq \mathbf{N}H_\pi$ folgt nach der Voraussetzung (c) auch $U^g \subseteqq \mathbf{N}A_\pi$.

Aus (d) *folgt* (a). Hierin liegt die Schwierigkeit. Sie wird durch 5.2 überwunden. Nach 5.2 genügt es nämlich zu zeigen, daß $H\mathbf{N}\pi A = G$ ist; es genügt also (weil $U^g \equiv G \bmod H$ vorausgesetzt ist) zu zeigen, daß es zu jedem $g \in G$ ein $h \in H$ derart gibt, daß $U^{gh} \subseteqq \mathbf{N}\pi A$ ist. Hierfür genügt $U^{gh} \subseteqq \mathbf{N}A_\pi$. Das wiederum ist nach Voraussetzung (d) gesichert, wenn wir $U^{gh} \subseteq \mathbf{N}H_\pi$ erreichen können. Nun gibt es aber nach der Voraussetzung (*) zu dem gegebenen g ein $h \in H$ derart, daß $H_\pi^{gh} = H_\pi$ ist. Für dieses h erhalten wir wegen $U \subseteqq \mathbf{N}H_\pi$ sofort $U^{gh} \subseteqq \mathbf{N}H_\pi^{gh} = \mathbf{N}H_\pi$. Damit ist der Beweis beendet.

Wir kommen nun zu der bisher aufgeschobenen Frage, wann Hallgruppen mit den benötigten Eigenschaften existieren. Wir geben zwei Sätze mit hinreichenden Bedingungen an.

5.4. *Sei* $A \in \mathbf{s}G$ *und* $H = \pi A^G$. *A enthalte eine* π*-Hallgruppe* A_π *mit einem Sylowturm (d. h.* A_π *besitze eine Normalkette, in der die Faktorgruppen je zweier benachbarter Glieder zu Sylowgruppen von A isomorph sind). Dann enthält H eine* π*-Hallgruppe* H_π *mit Sylowturm, für welche* $A \cap H_\pi = A_\pi$ *ist.*

Jede π*-Hallgruppe* H_π *von H, welche einen Sylowturm besitzt, erfüllt die Konjugiertheitsbedingung* 5.3*.

Beweis. Das Erzeugnis von subnormalen Untergruppen, von denen jede einen π-Hallgruppe mit Sylowturm (und zwar immer zur selben Anord-

nung der Primzahlen in der zugehörigen Normalkette) enthält, enthält ebenfalls eine π-Hallgruppe mit einem Sylowturm zur gleichen Anordnung der Primzahlen [6, Satz 3. 1]. Wendet man diesen Satz auf die sämtlichen Konjugierten von A in G an, so ergibt er die Existenz einer π-Hallgruppe H_π von H, welche einen Sylowturm mit der gleichen Anordnung wie A_π enthält. Nun ist $A \cap H_\pi$ eine π-Hallgruppe von A, welche einen Sylowturm von derselben Anordnung enthält wie die π-Hallgruppe A_π. Zwei solche Hallgruppen sind nach HALL [2, Th. A1] in A konjugiert. Wir können also $A_\pi = H_\pi$ annehmen, indem wir notfalls H_π durch eine geeignete konjugierte Gruppe ersetzen. Damit ist der erste Teil von 5.4 bewiesen. Der zweite Teil folgt unmittelbar aus dem eben erwähnten Satz von HALL.

5. 5. *Sei $A \in \mathfrak{s} G$ und $H = \pi A^g$. Es sei wenigstens eine der beiden folgenden Voraussetzungen erfüllt:*

(a) *Jede Kompositionsfaktorgruppe von A enthält eine nilpotente π-Hallgruppe.*

(b) *A enthält für die zu π komplementäre Primzahlmenge π' eine normale π'-Hallgruppe K derart, daß K oder A/K auflösbar ist.*

Behauptung: A enthält eine π-Hallgruppe. Zu jeder π-Hallgruppe A_π von A gibt es eine π-Hallgruppe H_π von H mit $A \cap H_\pi = A_\pi$. Jede π-Hallgruppe H_π von H erfüllt die Konjugiertheitsbedingung 5.3 *.

Beweis. (a) H ist das Erzeugnis der subnormalen Untergruppen πA^g ($g \in G$). Daher ist jede Kompositionsfaktorgruppe von H nach 2.4 zu einer geeigneten Kompositionsfaktorgruppe von πA isomorph, enthält also eine nilpotente π-Hallgruppe. Hieraus folgt nach HALL [2, Cor. D5. 1], daß H eine π-Hallgruppe H_π enthält und daß jede π-Untergruppe von H in einer passenden Konjugierten H_π^h enthalten ist. Wenn also A_π eine π-Hallgruppe von A ist (solche gibt es, z. B. $A \cap H_\pi$), so gibt es ein $h \in H$ mit $A_\pi \subseteq H_\pi^h$, also können wir durch Änderung der Bezeichnung $A_\pi \subseteq A \cap H_\pi$ erreichen. Da A_π und $A \cap H_\pi$ dieselbe Ordnung haben (auch $A \cap H_\pi$ ist nach 2.7 eine π-Hallgruppe von A), folgt $A_\pi = A \cap H_\pi$, wie gewünscht. Die gleiche Schlußweise zeigt, daß jede π-Hallgruppe von H die Bedingung 5.3 * erfüllt.

(b) Wir können ohne Beschränkung der Allgemeinheit annehmen, daß $A = \pi A$ ist, denn die Voraussetzungen über A übertragen sich unmittelbar auf πA. Wir zeigen zunächst, daß H eine normale π'-Hallgruppe L enthält, und zwar die Gruppe $L = \bigcup K^g$ ($g \in G$). Jedes K^g ist eine subnormale π'-Untergruppe von G (sogar von H wegen $K \subseteq A = \pi A$). Daher ist L nach 2.4 eine π'-Gruppe. Da andererseits $K = \pi' A$ ist, haben wir nach 2.6

$$L = \bigcup \pi' A^g = \pi' \bigcup A^g = \pi' H,$$

also ist L eine (und zwar die einzige) normale π'-Hallgruppe von H.

Jeder Kompositionsfaktor von H stimmt nach 2.4 mit einem Kompositionsfaktor einer Gruppe A^g überein, d. h. mit einem von A. Nach Voraussetzung (b) sind entweder alle durch Primfaktoren aus π' teilbaren Kompositionsfaktoren von A Primzahlen, oder alle durch Primfaktoren aus π teilbaren Kompositionsfaktoren von A sind Primzahlen. Das Gleiche gilt dann für H. Also ist entweder L oder H/L auflösbar. Wir fassen zusammen: H erfüllt die Voraussetzung, die in 5.5b für A formuliert war. Daraus folgt nach HALL [2, Th. D6, D7]: Es gibt in H eine π-Hallgruppe H_π derart, daß jede π-Untergruppe von H in einer passenden Konjugierten von H_π liegt. Nun können wir den Beweis wie im Fall (a) beenden.

Zum Schluß soll die Anwendung des Hauptsatzes an zwei Beispielen erläutert werden, deren einfachster Sonderfall ($\pi = p$) schon in der Einleitung erwähnt worden ist (1.1).

5.6. *Die subnormale Untergruppe A von G erfülle wenigstens eine der drei folgenden Bedingungen* (i)—(iii)*:*

(i) *A enthält eine π-Hallgruppe A_π mit Sylowturm,* (ii) 5.5a, (iii) 5.5b.

In den Fällen (ii) *und* (iii) *bezeichne A_π eine willkürlich gewählte π-Hallgruppe von A (solche gibt es nach* 5.5*).*

Behauptung: Genau dann ist πA eine charakteristische Untergruppe von G, wenn für jede Gruppe Γ von Automorphismen von G, für welche A_π^Γ eine π-Gruppe ist, $A_\pi^\Gamma = A_\pi$ gilt.

Beweis. Man kann den Hauptsatz 5.3 auf das Holomorph von G anwenden, d. i. die zerfallende Erweiterung von G mit der Gruppe aller Automorphismen von G. Für das U von 5.3b ist Γ einzusetzen.

5.7. *Sei $A \in \mathbf{s}G$. A erfülle wenigstens eine der beiden Bedingungen* 5.5a, 5.5b. *In G gebe es eine π-Hallgruppe G_π. Wir bilden $A \cap G_\pi = A_\pi$. Dann sind je zwei der folgenden drei Aussagen gleichwertig:*

(a) *πA ist normal in πG.*

(b) *Aus $g \in \pi G$ und $A_\pi \subseteq G_\pi^g$ folgt $A_\pi \in \mathbf{n} G_\pi^g$.*

(c) *Aus $g \in \pi G$, $A_\pi \subseteq P \in \mathbf{n} G_\pi$ und $P \in \mathbf{n} G_\pi^g$ folgt $A_\pi \in \mathbf{n} G_\pi^g$.*

Beweis. Aus (a) folgt (b). Denn aus $\pi G \subseteq \mathbf{N}\pi A$ und $A_\pi \subseteq G_\pi^g$ folgt $G_\pi^g \subseteq \pi G \subseteq \mathbf{N}\pi A$ und $A_\pi = \pi A \cap G_\pi^g$, also $G_\pi^g \subseteq \mathbf{N}A_\pi$.

Aus (b) folgt (c). Das ist trivial.

Aus (c) folgt (a). Wir können $G = \pi G$ annehmen. Sei $H = \pi A^G$. Wir setzen $H \cap G_\pi = H_\pi$. Dann ist H_π eine π-Hallgruppe von H. Ferner ist H_π normal in G_π, weil H normal in G ist. Nach 5.5 ist die Konjugiertheitsbedingung 5.3* erfüllt, und es ist $A \cap H_\pi = A_\pi$. Ferner ist die Voraussetzung

5. 3d erfüllt, wenn wir $U = G_{\pi'}$ wählen: Es ist $U^G = \pi' G = G$; und $U^g \subseteq \mathbf{N} H_{\pi'}$ bedeutet $H_{\pi'} \in \mathbf{n} G_{\pi'}^g$, also gilt nach der Voraussetzung 5. 7c, wenn wir sie auf $P = H_{\pi'}$ anwenden, $A_{\pi'} \in \mathbf{n} G_{\pi'}^g$, das heißt aber $U^g \subseteq \mathbf{N} A_{\pi'}$. Der Hauptsatz kann also angewendet werden und ergibt $\pi' G \subseteq \mathbf{N} \pi' A$, wie behauptet.

Literatur

[1] P. Hall, A contribution to the theory of groups of prime power order, *Proc. London Math. Soc.*, (2) **36** (1933), 29—95.

[2] P. Hall, Theorems like Sylow's, *Proc. London Math. Soc.*, (3) **6** (1956), 286—304.

[3] H. Wielandt, Eine Verallgemeinerung der invarianten Untergruppen, *Math. Zeitschr.*, **45** (1939), 209—244.

[4] H. Wielandt, Sylowgruppen und Kompositionsstruktur, *Abh. math. Sem. Univ. Hamburg*, **22** (1958), 215—228.

[5] H. Wielandt, Über den Normalisator der subnormalen Untergruppen, *Math. Zeitschr.*, **69** (1958), 463—465.

[6] H. Wielandt, Sylowtürme in subnormalen Untergruppen, *Math. Zeitschr.*, **73** (1960), 386—392.

(Eingegangen am 30. April 1960)

On inaccessible and minimal congruence relations. I

By G. GRÄTZER and E. T. SCHMIDT in Budapest

To professor Ladislaus Rédei on his 60th birthday

§ 1. Introduction

If we are given an abstract algebra A, then, partially ordering the set $\Theta(A)$ of all congruence relations of A under the usual rule: $\Theta \leqq \Phi$ if and only if $x \equiv y(\Theta)$ implies $x \equiv y(\Phi)$, $\Theta(A)$ becomes a complete lattice. It is customary to select two special types of congruence relations: the *inaccessible (from below)* congruence relations and the *minimal* ones. A congruence relation Θ is called inaccessible from below, if whenever the set $\{\Theta_\alpha\}$ of congruence relations is closed under finite joins, then $\Theta = \vee \Theta_\alpha$ implies $\Theta \in \{\Theta_\alpha\}$. A special type of inaccessible from below congruence relations is the minimal one: a congruence relation Θ is called minimal if there exists a pair of elements a, b of A, such that $a \equiv b(\Theta)$, and Θ is minimal with respect to this property. This Θ will be denoted by Θ_{ab}. (See [2] and [4].)

It is immediate from the definitions that the property of being inaccessible from below depends only on the structure of $\Theta(A)$, while the property of being minimal depends on the structure of A.

The minimal congruence relations are those which may be most easily described within A (see e. g. [3] and [5]). Further, the minimal congruence relations are those, which are closely connected with the elements of A. Therefore, in examining the structural properties of $\Theta(A)$, it seems to be useful to change A to an other abstract algebra $\bar{A}$ such that $\Theta(A) \cong \Theta(\bar{A})$ and in $\Theta(\bar{A})$ as many congruence relations are minimal as possible. Since the minimal congruence relations are inaccessible from below, further the property of being inaccessible from below is preserved under lattice isomorphisms, we see that at most the inaccessible from below congruence relations of A may become minimal (relative to $\bar{A}$).

The aim of the present note is to prove that this optimal case may always be achieved, that is, we prove the following

Theorem. *To any abstract algebra A there exists an abstract algebra $\bar{A}$ such that $\Theta(A) \cong \Theta(\bar{A})$ and in $\Theta(\bar{A})$ every inaccessible from below congruence relation is minimal (relative to $\bar{A}$).*

In the light of this theorem it seems to have some importance to characterize all abstract algebras $\bar{A}$ with the property stated in the theorem. In other words, given a class of abstract algebras, to determine all algebras of this class in which every inaccessible from below congruence relation is minimal.

This problem is extremely difficult, we do not hope a general solution of it. In the second part of this paper we shall solve it in the very special case of distributive lattices.

For the notions we will make use of we refer to [1].

§ 2. Preliminaries

In the proof of our Theorem we shall need two lemmata which will be proved in this section.

If A is an abstract algebra, then let $M(A)$ denote the set of all operations defined on A.

Lemma 1. *To any abstract algebra A one can find an abstract algebra A' such that $\Theta(A) \cong \Theta(A')$ and $M(A')$ consists of operations of one variable.*

Proof. We define an abstract algebra A' on the same set as A. Let $\varphi(x_1, \ldots, x_n)$ be an arbitrary operation of A. If $n > 1$ we may fix $n-1$ variables of $\varphi(x_1, \ldots, x_n)$, to get an operation $\varphi(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n)$ of a single variable x_i. We define the operations of A' as follows: they are the operations of one variable of A, further all the operations of one variable that have been made from the operations of more than one variable of A in all possible ways. It is easy to prove that $\Theta(A) \cong \Theta(A')$. Even more is true: if under the natural isomorphism $\Theta \to \bar{\Theta}$, then the congruence classes modulo Θ are indentical with the congruence classes modulo $\bar{\Theta}$.

Lemma 1 makes us possible to restrict ourselves to general algebras in which all the operations are of one variable.

Let us suppose that we are given a set of general algebras $\{B_\alpha\}$ satisfying the following axioms:

(A) the sets $\{B_\alpha\}$ form a chain, that is, given B_α and B_β, either $B_\alpha \subseteq B_\beta$ or $B_\beta \subseteq B_\alpha$, and in case $B_\alpha \subseteq B_\beta$ the operations of B_α are extended[1]) to B_β, which formally may be denoted by $M(B_\alpha) \subseteq M(B_\beta)$;

[1]) That is to any operation $\varphi(x)$ of B_α there exists an operation $\psi(x)$ of B_β such that $\varphi(a) = \psi(a)$ if $a \in B_\alpha$.

(*B*) if $B_\alpha \subseteq B_\beta$ and $\Theta \in \Theta(B_\alpha)$, then there is one and only one congruence relation $\bar{\Theta}$ of B_β such that $a \equiv b(\bar{\Theta})$ $(a, b \in B_\alpha)$ is equivalent to $a \equiv b(\Theta)$.

$\bar{\Theta}$ is called the congruence relation *induced* by Θ.

We define an abstract algebra $\bar{B}$ as follows: $x \in \bar{B}$ if $x \in B_\alpha$ for some α and $M(\bar{B}) = \bigvee_\alpha M(B_\alpha)$. From (*A*) it follows that $\bar{B}$ is an abstract algebra. Now we state

Lemma 2. *If the abstract algebra* $\bar{B}$ *is added to the set* $\{B_\alpha\}$ *then the arising set also satisfies the conditions* (*A*) *and* (*B*).

Proof. Condition (*A*) follows directly from the definition of $\bar{B}$. To prove (*B*) we take a B_α and a $\Theta \in \Theta(B_\alpha)$. Denote by Φ_β that congruence relation of $B_\beta \supseteq B_\alpha$ which is induced by Θ. We define $x \equiv y(\bar{\Theta})$ if and only if $x \equiv y(\Phi_\beta)$ for some β. It is easy to check that $\bar{\Theta}$ is a congruence relation of $\bar{B}$ and the only one having the property: $x \equiv y(\Theta)$ $(x, y \in B_\alpha)$ if and only if $x \equiv y(\bar{\Theta})$. Thus property (*B*) and so Lemma 2 is proved.

Corollary. *The isomorphism* $\Theta(B_\alpha) \cong \Theta(\bar{B})$ *holds for every* α.

§ 3. The construction of A_1

Let an abstract algebra A be given. We may suppose — owing to Lemma 1 — that all the operations of A are of one variable. We fix two elements a, b of A and construct an extension A_1 of A such that in A_1 every congruence relation of the form $\Theta_{ax} \cup \Theta_{by}$ is minimal and of course $\Theta(A) \cong \Theta(A_1)$.

To do this we define formally to every element $x \in A$ a symbol x^* subject to the sole rule: $a = b^*$. The set of all x^* is denoted by A^*. Thus $x \to x^*$ is a one-to-one correspondence between A and A^* and the only common element of A and A^* is a.

We consider the set $A_1 = A \cup A^*$ and define operations of one variable on this set.

1. The definition of $f(x)$: if $x \in A$, $f(x) = x^*$ and $f(x^*) = a^*$.
2. The definition of $g(x)$: if $x \in A$ then $g(x) = b$, and $g(x^*) = x$.
3. We extend all the operations $\omega(x)$ of A to A_1 by setting $\omega(x^*) = \omega(a)$.

$M(A_1)$ consists of the operations $f(x), g(x)$ and the $\omega(x)$ defined under 1—3. A_1 with the operations $M(A_1)$ is an abstract algebra.

We first prove $\Theta(A) \cong \Theta(A_1)$.

Let $\Theta \in \Theta(A)$ and define $u \equiv v(\bar{\Theta})$ if and only if one of the following conditions hold:

I. $u, v \in A$ and $u \equiv v(\Theta)$;

II. $u = x^*, v = y^*$ and $x \equiv y(\Theta)$;

III. $x \equiv a(\Theta)$, $b \equiv z(\Theta)$ and $u = x$ or $u = z^*$ and $v = x$ or $v = z^*$.

We show that the relation $\bar{\Theta}$ of A_1 is a congruence relation.

It is clear that $\bar{\Theta}$ is reflexive and symmetric. To show the transitivity of $\bar{\Theta}$ suppose that $u \equiv v(\bar{\Theta})$ and $v \equiv w(\bar{\Theta})$. If $u, v, w \in A$ or $u, v, w \in A^*$, then the transitivity (i. e. $u \equiv w(\bar{\Theta})$) is obvious. Consider the case $u, v \in A$ and $w \in A^*$ (the case $u \in A$ and $v, w \in A^*$ is quite similar). Then we have $u \equiv v(\Theta), v \equiv a(\Theta), x \equiv b(\Theta)$ where x is defined by $w = x^*$ (we get these by III and I), thus by the transitivity of Θ we get $u \equiv a(\Theta)$ and hence by III $u \equiv v(\bar{\Theta})$. It remained to consider the case $u, w \in A$ and $v \in A^*$ (the case $v \in A, u, w \in A^*$ may be discussed in the same way). From the assumptions, owing to III, we get $u \equiv a(\Theta), b \equiv x(\Theta), v = x^*, w \equiv a(\Theta), b \equiv x(\Theta)$ and the first and third of these congruences imply $u \equiv w(\Theta)$ what is (by I) the same as $u \equiv w(\bar{\Theta})$.

Now we prove for $\bar{\Theta}$ the substitution law. We have to show that $\psi(x) \in M(A_1)$ and $u \equiv v(\bar{\Theta})$ imply $\psi(u) \equiv \psi(v)(\bar{\Theta})$. We distinguish three cases:

a) $u, v \in A$. Then $f(u) \equiv f(v)(\bar{\Theta})$ by II. Concerning the operation $g(x)$ it results the trivial $g(u) = b \equiv b = g(v)(\bar{\Theta})$. If $\omega(x)$ is an operation of A which is extended to A_1, then $\omega(u) \equiv \omega(v)(\Theta)$, thus by I $\omega(u) \equiv \omega(v)(\bar{\Theta})$.

b) $u, v \in A^*$. Then $u = x^*, v = y^*$ and we have $x \equiv y(\Theta)$. Thus $x^* \equiv y^*(\bar{\Theta})$ and concerning the operation $f(x)$ we get $a^* \equiv a^*(\bar{\Theta})$. The operation $g(x)$ yields $x \equiv y(\bar{\Theta})$ which is by I also true. Finally, with an $\omega(x)$ we get $\omega(a) \equiv \omega(a)(\bar{\Theta})$ which is also trivial.

c) $u \in A$, $v \in A^*$. Then $v = x^*$ and the relations $u \equiv a(\Theta), b \equiv x(\Theta)$ are valid. From $u \equiv v(\bar{\Theta})$ we get concerning the operations $f(x), g(x)$ and $\omega(x)$ the following relations: $f(u) \equiv f(a)(\bar{\Theta}), b \equiv x(\bar{\Theta}), \omega(a) \equiv \omega(u)(\bar{\Theta})$ and all these relations are easy consequences of $u \equiv a(\Theta)$ and $b \equiv x(\Theta)$.

Hence we have proved that $\bar{\Theta}$ is a congruence relation. The following step is to show that the correspondence $\Theta \to \bar{\Theta}$ is an isomorphism between $\Theta(A)$ and $\Theta(A_1)$.

The congruence relation $\bar{\Theta}$ of A_1, induces in the natural way an equivalence relation on A which is just Θ. Since Θ completely determines $\bar{\Theta}$ the mapping $\Theta \to \bar{\Theta}$ is one-to-one from $\Theta(A)$ *into* $\Theta(A_1)$. It remains only to show that it is *onto*.

To do this suppose $\Phi \in \Theta(A_1)$. We define a relation Θ of A by $x \equiv y(\Theta)$ $(x, y \in A)$ if and only if $x \equiv y(\Phi)$. This Θ is a congruence relation of A and we prove $\bar{\Theta} = \Phi$. Since the laws I—III are consequences of the transi-

tivity of Θ alone and that of the substitution law, therefore $\bar{\Theta} \leqq \Phi$ is trivial. Thus we have to show only that every relation $u \equiv v(\Phi)$ follows from the relations of type $x \equiv y(\Theta)(x, y \in A)$, using the laws I—III. Let $u \equiv v(\Phi)$. If $u, v \in A$, then the assertion is trivial. It is also clear in case $u, v \in A^*$, for the validity of $x \equiv y(\Theta)$ is equivalent to that of $x^* \equiv y^*(\bar{\Theta})$. If $u \in A$ and $v \in A^*(v = x^*)$, then from $u \equiv v(\Phi)$ we get $u^* = f(u) \equiv f(v) = a^*(\Phi)$ and then $u = g(u^*) \equiv g(a^*) = a(\Phi)$. Thus $a \equiv v(\Phi)$ that is $b = g(a) \equiv g(v) = g(x^*) = x(\Phi)$. Thus we have under Θ the congruences $u \equiv a(\Theta)$ and $b \equiv x(\Theta)$ from which using the law III we get the required $u \equiv v(\Phi)$, as we wished to prove.

Summing up, $\Theta \to \bar{\Theta}$ is a one-to-one correspondence between $\Theta(A)$ and $\Theta(A_1)$, further, from the definition of $\bar{\Theta}$ it is clear that $\Theta > \Phi$ if and only if $\bar{\Theta} > \bar{\Phi}$. This implies that the correspondence in question is an isomorphism, thus

$$\Theta(A) \cong \Theta(A_1).$$

Secondly, we prove

$$\bar{\Theta}_{ax} \cup \bar{\Theta}_{by} = \bar{\Theta}_{xy^*}.$$

Indeed, $b \equiv y(\bar{\Theta}_{ax} \cup \bar{\Theta}_{by})$ and from this we obtain $a = b^* = f(b) \equiv f(y) = y^*(\bar{\Theta}_{ax} \cup \bar{\Theta}_{by})$ and comparing this with $x \equiv a(\bar{\Theta}_{ax} \cup \bar{\Theta}_{by})$ it results that $x \equiv y^*(\bar{\Theta}_{ax} \cup \bar{\Theta}_{by})$, that is, $\bar{\Theta}_{xy^*} \leqq \bar{\Theta}_{xa} \cup \bar{\Theta}_{by}$. Conversely, starting from $x \equiv y^*(\bar{\Theta}_{xy^*})$ we get $f(x) \equiv f(y^*) = a^*(\bar{\Theta}_{xy^*})$, that is, $x = g(f(x)) \equiv g(a^*) = a(\bar{\Theta}_{xy^*})$ and the transitivity implies $a = f(b) \equiv f(y)(\bar{\Theta}_{xy^*})$ and $b \equiv y(\bar{\Theta}_{xy^*})$, that is, $\bar{\Theta}_{ax} \cup \bar{\Theta}_{by} \leqq \bar{\Theta}_{xy^*}$, finishing the proof of the equality.

Thus A_1 has all the properties stated at the beginning of this section.

§ 4. The proof of the Theorem

Consider the abstract algebra A and define the set H as the set of all (unordered) pairs of the elements of A. We fix a well-ordering of H and to each $q_\alpha \in H$ we define an abstract algebra A_α in the following way: $A_0 = A$ where q_0 is the first element of H; if A_β is defined for all $\beta < \alpha$ then A_α is that general algebra which is constructed with the method of § 3 from $\bigcup_{\beta<\alpha} A_\beta$ if the fixed pair a, b of elements is just q_α.

We define the abstract algebra A^1 by

$$A^1 = \bigcup_\alpha A_\alpha.$$

We construct from A^1 an abstract algebra A^2 in the same way as A^1 was constructed from A, etc.

$$A \subseteq A^1 \subseteq \cdots \subseteq A^n \subseteq \cdots \qquad (n = 1, 2, \ldots)$$

Let $\bar{A}$ be the union of this chain of abstract algebras. We assert that the abstract algebra $\bar{A}$ fulfill the requirements of the Theorem.

First we prove $\Theta(A) \cong \Theta(A_\alpha)$ by transfinite induction on α. If this is true for all $\beta < \alpha$ and if $\alpha = \gamma + 1$, then the results of § 3 ensure $\Theta(A_\gamma) \cong \Theta(A_\alpha)$, the hypothesis implies $\Theta(A) \cong \Theta(A_\gamma)$ and thus $\Theta(A) \cong \Theta(A_\alpha)$. If α is a limit ordinal, then the Corollary of Lemma 2 together with the results of § 3 prove $\Theta(A) \cong \Theta(A_\alpha)$. Again, owing to Corollary of Lemma 2 we get $\Theta(A) \cong \Theta(A^1)$. In the same way we conclude that $\Theta(A) \cong \Theta(A^i)$ for all i, and again Corollary of Lemma 2 guarantees $\Theta(A) \cong \Theta(\bar{A})$.

Secondly, we prove that every inaccessible from below congruence relation of $\bar{A}$ is minimal. If this were not true, then there would exist an inaccessible from below congruence relation Φ of $\bar{A}$ which is not minimal; it may be supposed that Φ is of the form $\Phi = \Theta_{a_1 a_2} \cup \Theta_{a_3 a_4}$. The a_i-s are elements of $\bar{A}$ thus there exists an A^j containing all the a_i—s. From the construction of A^{j+1} it follows that Φ is minimal in A^{j+1}, thus in $\bar{A}$ too, a contradiction. Thus our Theorem is completely proved.

Bibliography

[1] G. Birkhoff, *Lattice theory* (New York, 1948).

[2] G. Birkhoff and O. Frink, Representations of lattices by sets, *Transactions Amer. Math. Soc.*, **64** (1948), 299—316.

[3] R. P. Dilworth, The structure of relatively complemented lattices, *Annals of Math.*, **51** (1950), 348—359.

[4] J. Hashimoto, Direct, subdirect decompositions and congruence relations, *Osaka Math. Journal*, **9** (1957), 87—117.

[5] А. И. Мальцев, К общей теории алгебраических систем, Мат. Сборник, **35** (1954), 3—20.

(Received May 2, 1960)

Über transfinite Funktionen. I

Von G. FODOR in Szeged

Herrn Professor László Rédei zum 60. Geburtstag gewidmet

Sei S eine Menge von der Mächtigkeit $\aleph_\alpha$ und $\mathrm{cf}(\alpha)>0$ (d. h. ω_α sei nicht mit ω konfinal). In S seien zwei Funktionen $f(x)$ und $\delta(x)$ mit Werten aus S bzw. $W(\omega_\alpha)=\{\beta:\beta<\omega_\alpha\}$ definiert, so daß $\delta(S)$ eine zusammengehörige Teilmenge von $W(\omega_\alpha)$ mit $0\in\delta(S)$ ist. Wir betrachten die folgenden Bedingungen A, B, und C:

A. Für alle $\gamma\in\delta(S)$, die Mächtigkeit der Menge $\delta^{-1}\gamma=\{x\in S:\delta(x)=\gamma\}$ ist kleiner als $\aleph_{\mathrm{cf}(\alpha)}$.

B. Für alle $x\in S$ mit $\delta(x)>0$, $\delta(f(x))<\delta(x)$ $(\delta(f(x))=\delta(x)$ für $\delta(x)=0)$ gilt.

C. Für alle $x\in S$, die Mächtigkeit der Menge $f^{-1}x=\{y\in S:f(y)=x\}$ ist kleiner als $\aleph_{\mathrm{cf}(\alpha)}$.

G. KUREPA hat den folgenden Satz bewiesen:

I. *Wenn* $\aleph_\alpha$ $(\alpha>0)$ *regulär ist, so folgt aus jeder zwei der Bedingungen* A, B *und* C, *die Negation der dritten.*

Nehmen wir an, daß S eine zusammengehörige Teilmenge von $W(\omega_\alpha)$ ist und seien A′ und C′ die folgenden Bedingungen:

A′. $\delta(x)$ ist bestimmt divergent,

C′. $f(x)$ ist bestimmt divergent.

Wir werden den folgenden Satz beweisen:

II. *Wenn* S *eine zusammengehörige Teilmenge von* $W(\omega_\alpha)$ *ist und* $\mathrm{cf}(\alpha)>0$ *gilt, so folgt aus jeder zwei der Bedingungen* A′, B *und* C′ *die Negation der dritten.*

Der Beweis des Satzes II zeigt, daß der Satz von KUREPA auch für singuläre $\aleph_\alpha$ mit $\mathrm{cf}(\alpha)>0$ gültig ist.

Es ist klar, daß A und A′ (bzw. C und C′) für reguläre $\aleph_\alpha$ gleichwertig sind. Für singuläre $\aleph_\alpha$ folgt aber weder A aus A′ (bzw. C aus C′) noch A′ aus A (bzw. C′ aus C).

Wir brauchen folgende Definitionen und Bezeichnungen (vgl. z. B. [2]). Ist A eine Ordnungszahl, so bedeute $W(A)$ die Menge aller Zahlen ξ, für die $\xi < A$ ist. Sind M und N zwei Teilmengen von $W(A)$ ohne Maximum, so heißen M und N zusammengehörig, wenn es zu jeder Ordnungszahl jeder der beiden Mengen eine größere Ordnungszahl in der anderen Menge gibt. Sind μ und ν zwei Limeszahlen, so heißt μ konfinal mit ν, wenn μ der Limes einer wachsenden Folge vom Typ ν ist. Ist α eine Limeszahl, so bedeute $\mathrm{cf}(\alpha)$ den Index der kleinsten Ordnungszahl ω_γ, mit der α konfinal ist. Eine auf einer mit $W(A)$ zusammengehörigen Teilmenge M von $W(A)$ definierte Funktion $\varphi(\xi)$ mit Werten aus $W(A)$ heißt bestimmt divergent, wenn es zu jedem $\alpha < A$ ein β gibt, so daß $\varphi(\xi) > \alpha$ für $\xi \geqq \beta$ gilt.

Wir beweisen nun den Satz II:

Beweis. Nehmen wir die Gültigkeit der Bedingungen B und C′ an. Wir beweisen, daß es sich hieraus die Negation der Bedingung A' ergibt. Daraus folgt leicht der Satz II.

Betrachten wir, für jedes $x \in S$, die Folge

$$f^0(x) = x,\ f^1(x) = f(x),\ f^2(x),\ \ldots, f^n(x), \ldots, \tag{1}$$

wobei $f^n(x) = f(f^{n-1}(x))$ $(n > 0)$ ist.

(i) Wenn eine Zahl l mit $m \leqq l < n$ existiert, für die $\delta(f^l(x)) \neq 0$ ist, so gilt

$$f^n(x) \neq f^m(x).$$

Wäre die Behauptung falsch, so ergäbe sich aus der Bedingung B, daß einerseits

$$\delta(f^m(x)) \geqq \delta(f^{m+1}(x)) \geqq \cdots \geqq \delta(f^l(x)) > \delta(f^{l+1}(x)) \geqq \cdots \geqq \delta(f^n(x)),$$

andererseits

$$\delta(f^n(x)) = \delta(f^m(x))$$

gilt, was unmöglich ist.

Daraus folgt, daß für jedes $x \in S$ eine nicht-negative Zahl n existiert, so daß $\delta(f^n(x)) = 0$ ist. Nehmen wir an, daß die Behauptung falsch ist. Dann ergibt sich aus B und (i), daß die Elemente der Folge (1) verschieden sind und

$$\delta(x) > \delta(f(x)) > \delta(f^2(x)) > \cdots > \delta(f^n(x)) > \cdots$$

besteht. Das ist aber eine Unmöglichkeit, weil jede absteigende Folge von Ordnungszahlen nur endlich viele Glieder enthält.

Für jedes $x \in S$ bezeichnen wir mit $n(x)$ die kleinste Zahl l, für die $\delta(f^l(x)) = 0$ ist. Es sei E eine zusammengehörige Teilmenge vom Typ $\omega_{\mathrm{cf}(\alpha)}$

von S. Jedem Element x von E entspricht also eine nicht-negative ganze Zahl $n(x)$. Es sei n eine solche Zahl und

$$E_n = \{x \in E : n(x) = n\}.$$

Da $\mathrm{cf}(\alpha) > 0$ und E eine zusammengehörige Teilmenge vom Typ $\omega_{\mathrm{cf}(\alpha)}$ von S ist, so existiert ein Index n_0, so daß E_{n_0} eine zusammengehörige Teilmenge von E ist.

Es sei $H = \delta(f^{n_0}(E_{n_0}))$. Offenbar ist $H = \{0\}$. Da E_{n_0} eine mit $W(\omega_\alpha)$ zusammengehörige Teilmenge von S ist, so folgt aus C', daß $f^{n_0}(E_{n_0})$ auch eine zusammengehörige Teilmenge von S ist. Daraus folgt, daß $\delta(x)$ nicht bestimmt divergent ist. Damit ist der Satz bewiesen.

Literatur

[1] G. Kurepa, On regressing functions, *Zeitschr. f. math. Logik und Grundlagen d. Math.*, 4 (1958), 148—156.

[2] H. Bachmann, *Transfinite Zahlen*, Ergebnisse der Math. und ihrer Grenzgebiete. Neue Folge, Heft 1 (Berlin—Heidelberg—Göttingen, 1955).

(Eingegangen am 27. Mai 1960)

Über gewisse spezielle kompatible Klasseneinteilungen von Halbgruppen

Von ISTVÁN PEÁK in Szeged

Herrn Prof. L. Rédei zum 60. Geburtstage gewidmet

Es sei $H = \alpha, \beta, \ldots$ eine Halbgruppe, d. h. eine nichtleere Menge, in der eine assoziative Multiplikation definiert ist. Wir beschäftigen uns mit einer besonderen Klasseneinteilung von H. Eine Klasseneinteilung C von H in die Klassen $C_1, C_2, \ldots$ wird kurz durch $H = C_1, C_2, \ldots$ bezeichnet. Die durch das Element $\alpha (\in H)$ repräsentierte Klasse C_i bezeichnen wir durch $C_i = C(\alpha)$.

Wir definieren die kompatible Klasseneinteilung einer Halbgruppe üblicherweise so:

Eine Klasseneinteilung C einer Halbgruppe H ist kompatibel, wenn die durch die Gleichung $C(\alpha)C(\beta) = C(\alpha\beta)$ definierte Klassenmultiplikation eindeutig ist.

Offenbar ist eine Klasseneinteilung C einer Halbgruppe H dann und nur dann kompatibel, wenn die zugehörige Äquivalenzrelation $\alpha \equiv \beta \Leftrightarrow C(\alpha) = C(\beta)$ eine Kongruenzrelation ist, d. h.

$$\alpha \equiv \beta \Rightarrow \varrho\alpha \equiv \varrho\beta, \quad \alpha\sigma \equiv \beta\sigma \qquad (\varrho, \sigma \in H).$$

Nach L. RÉDEI [2] nennen wir eine Unterhalbgruppe N einer Halbgruppe H mit Einselement ε, von der wir annehmen, daß sie ebenfalls ε zum Einselement hat, *linksnormal,* wenn eine kompatible Klasseneinteilung von H von der Form

$$H = N, \ \alpha N, \ \beta N, \ \ldots \tag{1}$$

existiert. (Die ursprüngliche Definition von L. RÉDEI hat wegen der Anwendung auf das Schreiersche Erweiterungsproblem auch die Einschränkung enthalten, daß jedes Produkt αN schlicht (vgl. RÉDEI [3]) ist, d. h. $\alpha\nu_1 = \alpha\nu_2$ $(\alpha \in H, \ \nu_1, \nu_2 \in N)$ nur im Falle $\nu_1 = \nu_2$ gilt. Wir haben diese zusätzliche einschränkende Bedingung fallen lassen.) Entsprechend versteht man die *rechtsnormale* Unterhalbgruppe von H. Nach R. WIEGANDT [4] nennen wir eine

Unterhalbgruppe N von H *normal,* wenn N links- und rechtsnormal in H ist. WIEGANDT [4] hat die folgenden zwei Behauptungen bewiesen. Erstens, wenn N eine normale Unterhalbgruppe einer Halbgruppe H mit Einselement ist, dann sind die linksseitige Klasseneinteilung (1) und die entsprechende rechtsseitige Klasseneinteilung $H=N, N\varrho, N\sigma, \ldots$ übereinstimmend. Zweitens, wenn $\alpha(\in H)$ sein Inverses in H hat, dann ist $\alpha N=N\alpha$.

Wir geben eine Ergänzung dieser Resultate für den Fall, daß N eine Gruppe ist.

Im folgenden sei H immer eine Halbgruppe mit Einselement ε und N eine Untergruppe von H, die das Einselement von H enthält. Es ist bekannt, daß die sämtlichen verschiedenen Untermengen von der Form αN $(\alpha \in H)$ eine Klasseneinteilung von H bilden (s. RÉDEI [3]). Leicht folgt ferner (s. WIEGANDT [4]), daß jetzt für jede Klasse αN und für ihre sämtlichen Elemente α' $(\in \alpha N)$ die Gleichung $\alpha' N=\alpha N$ gilt. Die Klasseneinteilung

$$H=N,\ \alpha N,\ \beta N,\ \ldots \tag{2}$$

von H nennen wir jetzt die *linksseitige Klasseneinteilung von H nach N.* Im folgenden interessieren wir uns nur für die Klasseneinteilungen dieser Art.

Satz 1. *Es sei N eine Untergruppe einer Halbgruppe H mit Einselement ε, die das Einselement von H enthält. Dann sind die folgenden Behauptungen äquivalent:*

(A) *N ist linksnormal in H,*

(B) *$\alpha N=N\alpha$ gilt für jedes $\alpha(\in H)$,*

(C) *die linksseitige und rechtsseitige Klasseneinteilungen von H nach N sind übereinstimmend,*

(D) *N ist rechtsnormal in H.*

Beweis. (A)$\Rightarrow$(B): Ist N linksnormal in H, so ist die Klasseneinteilung $H=N, \varrho N, \sigma N, \ldots$ kompatibel und die zugehörige Äquivalenzrelation ist eine Kongruenzrelation. Für $\alpha(\in H)$, $\nu(\in N)$ gilt $\nu\equiv\varepsilon$, also auch $\nu\alpha\equiv \equiv\varepsilon\alpha\equiv\alpha\varepsilon$. Daraus folgt $\nu\alpha\in\alpha N$ d. h. $N\alpha\subseteq\alpha N$. Ähnlich erhalten wir $\alpha N\subseteq N\alpha$, also $\alpha N=N\alpha$.

(B)$\Rightarrow$(C): Diese Behauptung ist trivial.

(C)$\Rightarrow$(A): Wenn die Klasseneinteilungen $H=N, \alpha N, \beta N, \ldots$ und $H=N, N\varkappa, N\lambda, \ldots$ übereinstimmend sind, existiert für jedes αN ein $\nu(\in H)$ mit $\alpha N=N\nu$. Dann gilt wegen $\alpha\in N\nu$ auch $N\alpha=N\nu$, also $\alpha N=N\alpha$ für jedes $\alpha(\in H)$. Wir zeigen, daß die zur Klasseneinteilung $H=N, \alpha N, \beta N, \ldots$ gehörige Äquivalenzrelation eine Kongruenzrelation ist. Hierzu betrachten wir eine Äquivalenz $\varrho\equiv\sigma\Leftrightarrow\varrho N=\sigma N$. Für jedes $\mu(\in H)$ gilt $\mu\varrho N=\mu\sigma N$,

d. h. $\mu\varrho \equiv \mu\sigma$. Da $\alpha N = N\alpha$ $(\alpha \in H)$ ist, folgt noch $\varrho\mu N = \varrho N\mu = \sigma N\mu = \sigma\mu N$ also $\varrho\mu \equiv \sigma\mu$.

Wegen der Symmetrie der Voraussetzungen (B) und (C) sind die Implikationen (D) $\Rightarrow$ (B) und (C) $\Rightarrow$ (D) ähnlich ableitbar. Damit ist der Satz bewiesen.

Die Menge der Klassen von der Form αN $(\alpha \in H)$ von H nach N bezeichnen wir durch H/N. Definieren wir die Multiplikation in H/N durch die Gleichung $\alpha N \cdot \beta N = \alpha\beta N$, so ist H/N eine Halbgruppe, die wir, wie es üblich ist, die Faktorhalbgruppe von H nach N nennen.

Wir beweisen leicht noch den folgenden

Satz 2. *Enthalten die Untergruppen M, N einer Halbgruppe H das Einselement ε von H und sind sie linksnormal in H, so ist MN und im regulären Fall*[1]*) auch $M \cap N$ linksnormal in H.*

Beweis. Nach Satz 1 gilt $MN = NM$. Daraus folgt $(MN)^2 = MNMN = M^2N^2 = MN$ und ersichtlich $\varepsilon \in MN$. Anderseits ist $\nu^{-1}\mu^{-1}$ $(\nu \in N, \mu \in M)$ wegen $NM = MN$ ein Element von MN und dies ist das Inverse von $\mu\nu (\in MN)$ in MN.[2]) Also ist MN eine Untergruppe von H mit Einselement ε. Wegen $\varrho MN = M\varrho N = MN\varrho$ $(\varrho \in H)$ ist MN linksnormal in H.

Der Durchschnitt $M \cap N$ der Gruppen M, N ist auch eine Gruppe und $\varepsilon \in M \cap N$. Für ein reguläres H ist wegen $\varrho(M \cap N) = \varrho M \cap \varrho N = M\varrho \cap N\varrho = (M \cap N)\varrho$ auch $M \cap N$ linksnormal in H. Damit haben wir den Beweis des Satzes beendet.

Für die Halbgruppen mit Einselement hat E. S. Ljapin [1] den Begriff der normalen Unterhalbgruppe folgenderweise eingeführt. Es sei H eine Halbgruppe mit Einselement und N eine Unterhalbgruppe von H, die das Einselement von H enthält. N ist normal im Sinne von Ljapin in H, wenn für beliebige Elemente $\alpha, \beta (\in H)$, $\nu (\in N)$

$$\alpha\nu\beta \in N \Leftrightarrow \alpha\beta \in N$$

erfüllt. Wir bemerken, daß eine das Einselement von H enthaltende, im Sinne von Rédei normale Untergruppe von H auch im Sinne von Ljapin normal ist. Wirklich, seien $\alpha, \beta \in H$, $\nu \in N$ und $\alpha\nu\beta \in N$, dann gibt es nach Satz 1 ein Element $\mu (\in N)$ mit $\alpha\nu\beta = \mu\alpha\beta$ und auch $\alpha\beta = \varepsilon\alpha\beta = \mu^{-1}\mu\alpha\beta = \mu^{-1} \cdot \alpha\nu\beta \in N$ (μ^{-1} bedeutet das Inverse von μ in der Gruppe N) gilt. Umgekehrt, nehmen wir an, daß $\alpha\beta \in N$ ist und sei $\nu \in N$. Dann gibt es $\nu' (\in N)$ mit $\alpha\nu\beta = \nu'\alpha\beta$, daraus folgt $\alpha\nu\beta \in N$. Also ist N tatsächlich normal auch im Sinne von Ljapin.

---

[1]) Regulär heißt eine Halbgruppe, in der die Kürzungsregeln gelten.

[2]) μ^{-1} und ν^{-1} bedeuten das Inverse von μ bzw. ν in der Gruppe M bzw. N.

Es sei N eine Untergruppe der Halbgruppe H mit Einselement, die das Einselement von H enthält und normal im Sinne von RÉDEI ist. Nach LJAPIN [1] definieren wir in H die folgende Relation: Es gelte $\varrho \sim \sigma$ dann und nur dann, wenn $\mu, \mu' (\in N)$ mit $\varrho\mu = \mu'\sigma$ existieren. Wir zeigen, daß die zur Relation $\varrho \sim \sigma$ gehörige Klasseneinteilung von H und die Klasseneinteilung von H nach N übereinstimmen. Es sei, nämlich $\varrho \equiv \sigma \Leftrightarrow \varrho, \sigma \in \alpha N$. Dann gibt es Elemente $\nu, \nu' (\in N)$ mit $\varrho = \alpha\nu$, $\sigma = \alpha\nu'$. Sei $\varkappa \in N$ mit $\nu = \varkappa\nu'$, dann gilt $\varrho\varepsilon = \varrho = \alpha\nu = \alpha\varkappa\nu' = \varkappa'\alpha\nu' = \varkappa'\sigma$ $(\varkappa' \in N)$ und somit ist $\varrho \sim \sigma$. Umgekehrt, nehmen wir an, daß $\varrho \sim \sigma$ gilt, d. h. existieren $\varkappa, \lambda (\in N)$ mit $\varrho\varkappa = \lambda\sigma$. Dann gilt $\sigma = \lambda^{-1}\varrho\varkappa = \varrho\tau\varkappa$ $(\tau \in N)$ und daraus folgt $\sigma \in \varrho N$, ist also $\varrho \equiv \sigma$ erfüllt.

Aus diesen und aus den Sätzen 3. 7 und 5. 1 von LJAPIN [1] erhalten wir die

Folgerung. *Durchläufe N die Menge der (im Sinne von* RÉDEI*) normalen Untergruppen*[3]*) der Halbgruppe H mit Einselement, die das Einselement von H enthalten. Dann entweder gibt es keine Gruppe unter den Faktorhalbgruppen H/N der Halbgruppe H, oder ist jede Faktorhalbgruppe H/N eine Gruppe.*

Literaturverzeichnis

[1] Е. С. Ляпин, Ядра гомоморфизмов ассоциативных систем, Мат. сборник, **20 (62)** (1947), 497—514.

[2] L. RÉDEI, Die Verallgemeinerung der Schreierschen Erweiterungstheorie, *Acta Sci. Math.*, **14** (1952), 252—273.

[3] L. RÉDEI, *Algebra.* I (Leipzig, 1959), Satz 69, Seite 127.

[4] R. WIEGANDT, On complete semi-groups, *Acta Sci. Math.*, **19** (1958), 93—97.

(Eingegangen am 22. Februar 1960)

[3]) D. h. N ist eine normale Unterhalbgruppe von H, die gleichzeitig eine Gruppe ist.

Bemerkung über die einstufig nichtregulären Ringe

Von RICHARD WIEGANDT in Orosháza (Ungarn)

Herrn Professor L. Rédei zum 60. Geburtstag gewidmet

Professor RÉDEI hat in seiner Arbeit [1] die einstufig nichtregulären Ringe definiert und charakterisiert. Nach ihm nennen wir einen Ring einstufig nichtregulär, wenn er nichtregulär ist und seine echten Unterringe regulär sind. (Regulär heißt ein Ring, wenn er nullteilerfrei ist.) Die sämtlichen einstufig nichtregulären Ringe sind nach [1] die Zeroringe von Primzahlordnung und die direkten Summen von zwei endlichen Primkörpern.

Auf Grund dieses Ergebnisses können wir die einstufig nichtregulären Ringe auch anders charakterisieren.

Satz 1. *Für jeden Ring R sind die folgenden drei Bedingungen äquivalent:*

(1) *R ist einstufig nichtregulär,*

(2) *R ist kein Schiefkörper und die sämtlichen echten Unterringe von R sind Schiefkörper,*

(3) *R ist ein Zeroring von Primzahlordnung oder die direkte Summe von zwei endlichen Primkörpern.*

Zu dem Beweis gebrauchen wir den folgenden

Satz 2. *Für jeden Ring R sind die folgenden zwei Bedingungen äquivalent:*

(a) *R ist kein Schiefkörper und jedes echte Linksideal von R ist ein Schiefkörper,*

(b) *R ist ein Zeroring von Primzahlordnung oder die direkte Summe von zwei Schiefkörpern.*

Außerdem beweisen wir den folgenden

Satz 3. *Für einen Artinschen Ring R (d. h. R erfüllt die Minimalbedingung für die Linksideale) sind die folgenden drei Bedingungen äquivalent:*

(1°) *R ist nichtregulär und jedes echte Linksideal von R ist regulär,*

(2°) *R ist kein Schiefkörper und jedes echte Linksideal von R ist ein Schiefkörper,*

(3°) *R ist ein Zeroring von Primzahlordnung oder die direkte Summe von zwei Schiefkörpern.*

Zuerst beweisen wir Satz 2. Aus Bedingung (b) folgt (a) unmittelbar. Umgekehrt, nehmen wir an, daß der Ring R die Bedingung (a) erfüllt. Dann ist R ein Artinscher Ring.

Es bezeichne n das Radikal von R. Nur die Fälle $n = R, 0$ sind möglich, denn sonst wäre n ein echtes Linksideal von R mit lauter nilpotenten Elementen, entgegen der Voraussetzung.

Im Fall $n = R$ sind alle Elemente von R nilpotent. Wegen der Annahme enthält dann der Ring R keine echten Linksideale, also ist der Ring R nach einem Satz von T. SZELE [2] ein Zeroring von Primzahlordnung.

Im Fall $n = 0$ ist R halbeinfach, also gilt nach dem Satz von WEDDERBURN—ARTIN eine Zerlegung

$$R = S_1 + \cdots + S_k \qquad (k \geqq 1)$$

in eine direkte Summe von vollen Matrixringen $S_1, \ldots, S_k$ über Schiefkörpern. Jedoch müssen diese Matrixringe den Rang 1 haben, d. h. lauter Schiefkörper sein, denn sonst hätte R echte Linksideale mit Nullteilern. Da ferner R nullteiler hat, so muß $k > 1$ sein. Da die echten Linksideale von R nullteilerfrei sind, so muß $k = 2$ bestehen. Damit haben wir Satz 2 bewiesen.

Jetzt können wir schon Satz 1 beweisen. Nach dem Satz von RÉDEI [1] sind die Bedingungen (1) und (3) äquivalent. Wir zeigen aus, daß die Bedingungen (2) und (3) auch äquivalent sind.

Aus (3) folgt (2) unmittelbar. Umgekehrt, nehmen wir an, daß der Ring R die Bedingung (2) erfüllt. Da die echten Linksideale von R Schiefkörper sind, so ist R wegen Satz 2 ein Zeroring von Primzahlordnung oder die direkte Summe von zwei Schiefkörpern S_1, S_2. Wegen der Voraussetzung sind die echten Unterringe von R nullteilerfrei, also müssen die Schiefkörper S_1, S_2 endliche Primkörper sein. Somit ist der Satz bewiesen.

Endlich beweisen wir Satz 3. Wegen Satz 2 sind die Bedingungen (2°) und (3°) äquivalent, ferner folgt (1°) aus (3°) trivial. Umgekehrt nehmen wir die Bedingung (1°) an. Jetzt muß das Radikal n von R entweder R oder 0 sein. Wegen der Annahme kann der Ring R im Fall $n = R$ keine echten Linksideale enthalten, also ist R ein Zeroring von Primzahlordnung. Im Fall $n = 0$ ist R halbeinfach, also gilt eine Zerlegung

$$R = T_1 + \cdots + T_n \qquad (n \geqq 1)$$

in eine direkte Summe von vollen Matrixringen $T_1, \ldots, T_n$ über Schiefkörpern. Diese Matrixringe müssen Schiefkörper sein, denn sonst hätte R echte Linksideale mit Nullteilern. Da R Nullteiler hat, so muß $n>1$ sein. Da die echten Linksideale von R regulär sind, muß $n=2$ sein. Damit ist der Satz bewiesen.

Literaturverzeichnis

[1] L. Rédei, Die einstufig nichtregulären Ringe, *Acta Sci. Math.*, **20** (1959), 238—244.
[2] T. Szele, Die Ringe ohne Linksideale, *Buletin Ştiinţific Bucureşti*, **1** (1949), 783—789.

(Eingegangen am 19. Februar 1960)

Bibliographie

Hans Richter, Wahrscheinlichkeitstheorie (Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen, Bd. 86), XII + 435 Seiten, Berlin—Göttingen—Heidelberg, Springer-Verlag, 1956.

Before the publication of this work there was no text-book in German introducing the reader to modern probability theory. The main purpose of the author was to fill this gap. Thus he mainly aims at discussing the fundamental chapters of the theory.

His book differs from other books on probability before all in paying special attention to the connection between the mathematical and intuitive concept of probability. The second and a part of the third chapter are devoted to this question. Chapter 3 deals also with conditional probability, BAYES' theorem and some other notions.

From Chapter 5 on the book is based entirely on measure theory. (All what is necessary from measure theory and integration theory is expounded in chapters 1 and 4.) Chapter 5 deals with random variables, distribution and density functions, characteristic functions etc. Chapter 6 is devoted to special distributions, especially to those occuring in mathematical statistics. In Chapter 7 theorems concerning sequences of independent random variables, as the zero-one law the laws of large numbers, the law of iterated logarithm and the central limit theorem is discussed.

The whole book is written in a very precise form. It contains also some excercises together with their solutions.

P. Révész (Budapest)

C. F. Gauß, Gedenkband anläßlich des 100. Todestages am 23. Februar 1955. Herausgegeben von H. REICHARDT. III + 251 Seiten, Leipzig, Teubner Verlag, 1957.

Die Herausgeber haben sich das Ziel gesetzt, die Universalität des Genies von GAUSS in mehreren unabhängigen, sich mit Hauptgebieten des Gaußschen Lebenswerkes beschäftigenden Abhandlungen darzustellen. Es folgen nach einem Vorwort und einführenden bzw. historischen allgemeinen Betrachtungen weitere neun Essais über die Arbeiten in Bezug auf Zahlentheorie, Algebra, Differentialgeometrie, Grundlagen der Geometrie, Funktionentheorie, reelle Analysis, Wahrscheinlichkeitsrechnung, Astronomie und Geodäsie, einige Teile der Physik — aus den Federn deutscher und sowjetischer Mathematiker.

Die Prachtausstellung ist dem Anlaß und dem reichen, gut illustrierten Inhalt des Bandes angemessen.

Miklós Mikolás (Budapest)

Loo-keng Hua, Additive Primzahltheorie, VI + 174 Seiten, Leipzig, Teubner Verlagsgesellschaft, 1959.

Das vorliegende Buch ist der Untersuchung des Waring—Goldbachschen Problems und eines verwandten Gleichungssystems mit Primzahlen als Unbekannten von speziellem Charakter gewidmet.

Im ersten, größeren Teil des Buches — in zehn Kapiteln von zwölf — wird das Waring—Goldbachsche Problem betrachtet. Verf. stellt, mit Hilfe eines, dem Leser ohne Beweis mitgeteilten, Siegel—Walfiszschen Satzes, für die Anzahl der Lösungen des genannten Problems eine asymptotische Formel auf. Das Hauptglied dieser Formel enthält als einen Faktor die singuläre Reihe. Die eigentliche Schwierigkeit liegt im Nachweis der Positivität dieser Reihe. Verf. zeigt, daß im Spezialfall $f(x) \equiv x^k$ die singuläre Reihe positiv ist. Dadurch wird es ihm ermöglicht, eine Menge wichtiger Folgerungen abzuleiten, von denen wir nur den bekannten Satz von Vinogradov hervorheben möchten, laut dessen sich jede hinreichend große ungerade Zahl als eine Summe von drei Primzahlen darstellen läßt.

In nachstehenden Kapiteln des Buches werden die gewonnenen Resultate durch stärkeren ersetzt. Um jene zu erzielen, führt Verf. den Begriff der exponentiellen Dichte ein. Mit Hilfe dieser kann man auf $H(k) \sim 4k \log k$ schließen, wo $H(k)$ die kleinste natürliche Zahl s von der Beschaffenheit bedeutet, daß jede hinreichend große Zahl einer arithmetischen Progression, deren Differenz von k abhängt, eine Summe von s k-ten Primzahlpotenzen ist.

Die zwei letzten Kapitel behandeln das erwähnte Gleichungssystem. Verf. zeigt, daß es stets eine Lösung in Primzahlen besitzt, wenn nur „die Bedingung der Lösbarkeit in positiven Zahlen" nebst „der Bedingung der Lösbarkeit als Kongruenz" erfüllt sind. Man überzeugt sich leicht, wie Verf. bemerkt, daß auch Gleichungssysteme von viel allgemeinerem Charakter mit Hilfe der verwendeten Methoden sich behandeln lassen.

Verf. baut sein Buch ohne Benützung analytischer Hilfsmittel auf. Das gelingt ihm durch Verwendung des erwähnten Siegel—Walfiszschen Satzes. Die Resultate, die im Buche dargestellt sind, stammen hauptsächlich vom Verf. selbst, und sind durch die vom Verf. verschärften Methode von Vinogradov erzielt.

Diese Monographie von Loo-keng Hua ist ein sehr anregendes Lesestück und ein wahrer Gewinn für die mathematische Literatur.

K. Corrádi (Budapest)

Proceedings of the International Congress of Mathematicians, 14—21 August 1958, edited by **J. A. Todd,** F. R. S., LXIV + 573 pages, University Press, Cambridge, 1960.

The volume contains the official record of the 1958 Congress in Edinburgh, including the reports on the work of the two Fields medallists of the Congress: K. F. Roth and R. Thom (written by H. Davenport and H. Hopf, respectively). It follows the text of addresses given by invitation of the Programme Committee: 17 one-hour and 34 half-hour addresses (of the 19 + 37 read at the Congress). Short communications, read in the section meetings, are mentioned only by title: abstracts of them were printed in a volume issued to members during the Congress.

On the whole, the volume gives an impressive cross-section of the immense variety, and at the same time of the unity, of present day mathematical research work done throughout the world.

Béla Sz.-Nagy (Szeged)

Paul B. Fischer †, Arithmetik, 3. Auflage (Sammlung Göschen, Band 147), 152 Seiten, Berlin, Walter de Gruyter & Co., 1958.

Obwohl die erste Auflage dieses Büchleins 1938 erschienen ist, ist es auch noch heute ein nützliches Lehrbuch, welches u. a. einen Überblick über die Geschichte und eine systematische Entwicklung der Zahlenbegriffe gibt, die Quaternionen mit inbegriffen. In einem Anhang werden die arithmetischen und geometrischen Reihen, die Zinseszins- und Rentenrechnung, und die Elemente der Kombinatorik behandelt.

J. Szendrei (Szeged)

Friedrich Bachmann, Aufbau der Geometrie aus dem Spiegelungsbegriff (Grundlehren der math. Wissenschaften in Einzeldarstellungen, Bd. 96), XIV + 311 Seiten, mit 160 Abbildungen, Berlin—Göttingen—Heidelberg, Springer-Verlag, 1959.

Nach dem Vorwort des Buches wird in diesen Vorlesungen „ein Aufbau der *ebenen metrischen Geometrie* entwickelt, bei dem von den Spiegelungen und der von den Spiegelungen erzeugten *Bewegungsgruppe* systematisch Gebrauch gemacht wird". Der Urkeim dieses Gedankens ist in den von J. Bolyai stammenden *absoluten Sätzen* enthalten. Seine Ausarbeitung begann jedoch erst mit dem 1907 publizierten berühmten Werke von J. Hjelmslev, in dem die Spiegelung bei der Grundlegung der Geometrie eine führende Rolle erhielt. Das Bestreben zu einer Verknüpfung der Theorie der Bewegungsgruppen der Ebene mit der Hjelmslevschen Grundlegung, sowie das Bestreben zu Verallgemeinerungen wurde während eines halben Jahrhunderts zur Quelle einer ausgedehnten Literatur. Das vorliegende Buch kann — abgesehen von einigen neueren noch offenen Fragen — als ein Schlußstein zu dieser Literatur angesehen werden.

Der Gedankengang der Grundlegung der metrischen Geometrie in diesem Werke ist der folgende:

Die metrische Ebene ist die Gesamtheit von Punkten und Geraden, die ein Axiomensystem A befriedigen. Das vom Verfasser angegebene Axiomensystem besteht aus Axiomen der Inzidenz, der Orthogonalität und der Spiegelung, insgesamt aus $3+3+2=8$ Axiomen. Die Abbildungen einer metrischen Ebene auf sich, die als Produkte von Spiegelungen auf Geraden darstellbar sind, werden Bewegungen genannt; ihre Gruppe heißt die Bewegungsgruppe der metrischen Ebene.

Man betrachte eine (abstrakte) Gruppe $\mathfrak{G}$, die ein aus involutorischen Elementen bestehendes invariantes Erzeugendensystem $\mathfrak{S}$ hat, und die Menge $\mathfrak{U}$ aller involutischer Elemente von $\mathfrak{G}$, die als Produkte von zwei Elementen aus $\mathfrak{S}$ darstellbar sind. Der Autor gibt ein aus 5 Axiomen bestehendes Axiomensystem B, betreffend die Elemente von $\mathfrak{S}$ und $\mathfrak{U}$, und betrachtet die Gruppen, in denen diese Axiome gelten. Ist insbesondere $\mathfrak{G}$ die Bewegungsgruppe einer dem Axiomensystem A genügenden Ebene, so genügt sie auch dem Axiomensystem B, wenn für $\mathfrak{S}$ die Gesamtheit der Geradenspiegelungen genommen wird; $\mathfrak{U}$ ist dabei die Gesamtheit der Punktspiegelungen. Aus diesem Grund nennt man die Elemente von $\mathfrak{S}$ bzw. $\mathfrak{U}$ auch im allgemeinen *Geraden-* bzw. *Punktspiegelungen.*

Die durch B bestimmte Theorie nennt der Autor die *ebene metrische Geometrie.* Da dieses Axiomensystem keine besondere Forderung über die Parallelität enthält, benützt der Autor auch die Benennung: *ebene absolute Geometrie.* Diese Geometrie ist aber von wesentlich allgemeinerer Natur, als die absolute Geometrie im klassischen Sinne und, da sie auch die Axiome der Anordnung und die Postulation der freien Beweglichkeit vermeidet, gestattet auch Ebenen, die aus Punkten und Geraden in endlicher Anzahl bestehen. Die absolute Ebene kann mittels Einführung von weiteren Axiomen derart spezialisiert werden, daß die euklidische, die hyperbolische, bzw. die elliptische Geometrie gewonnen wird.

Hierauf beweist der Autor, daß jede metrische Ebene in eine sogenannte *projektiv-metrische Ebene* eingebettet werden kann. Die Begründung der ebenen metrischen Geometrie erhält einen Abschluß durch das *Haupt-Theorem:* Die Bewegungsgruppen, welche dem Axiomensystem B genügen, sind als Untergruppen von Bewegungsgruppen projektiv-metrischer Ebenen darstellbar.

Wir wollen den reichen Inhalt des Buches nicht weiter detaillieren, nur zählen wir zur Orientierung die Titel der Kapitel auf: I. Einführung, II. Metrische (absolute) Geometrie, III. Projektiv-metrische Geometrie, IV. Euklidische Geometrie, V. Hyperbolische Geometrie, VI. Elliptische Geometrie. Wir erwähnen noch, daß im Anhang des Buches auch einige bis heute offene Problemkreise (besonders das Umkehrproblem des Haupt-Theorems) skizziert werden.

Franz Kárteszi (Budapest)

LIVRES REÇUS PAR LA RÉDACTION

H. Arzeliès, Milieux conducteurs ou polarisables en mouvement, XLIV + 347 pages, Paris, Gauthier-Villars, 1959. — 58 NF

N. Bourbaki, Eléments de mathématique XXVI, Groupes et algèbres de Lie, Chapitre I: **Algèbres de Lie** (Actualités sci. et ind., 1285), 142 pages, Paris, Hermann, 1960. — 21 NF

J. W. S. Cassels, An Introduction to the Geometry of Numbers (Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Bd. 99), VIII + 344 Seiten, Berlin—Göttingen—Heidelberg, Springer-Verlag, 1959. — DM 69, —

R. Garnier, Cours de mathématiques générales, Tome IV, VI + 275 pages, Paris, Gauthier-Villars, 1959. — 45 NF

J. Horn—H. Wittich, Gewöhnliche Differentialgleichungen, 6. Auflage (Göschens Lehrbücherei, I. Gruppe, Reine und angewandte Mathematik, Bd. 10), 275 Seiten, Berlin, Walter de Gruyter & Co., 1960. — DM 32, —

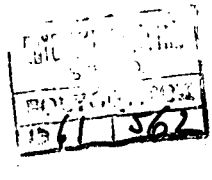
D. A. Kappos, Strukturtheorie der Wahrscheinlichkeitsfelder und -Räume (Ergebnisse der Mathematik und ihrer Grenzgebiete, neue Folge, Heft 24), IV + 136 Seiten, Berlin—Göttingen—Heidelberg, Springer-Verlag, 1960. — DM 21,80

H. Meschkowski, Ungelöste und unlösbare Probleme der Geometrie, VIII + 168 Seiten, Braunschweig, F. Vieweg, 1960. — DM 19,80

A. Monjallon, Introduction aux mathématiques modernes, 180 pages, Paris, Librairie Vuibert, 1960. — 20 NF

Proceedings of Symposia in Applied Mathematics, Vol. 9, **Orbit Theory,** edited by **G. Birkhoff** and **R. E. Langer,** V + 195, Providence, American Mathematical Society, 1959. — $ 7,20

O. Zariski, Introduction to the Problem of Minimal Models in the Theory of Algebraic Surfaces (Publications of the Mathematical Society of Japan, No. 4), VII + 89, Tokyo, The Mathematical Society of Japan, 1958. —



Le fascicule prochain contiendra entre autres les articles suivants dédiés au 60ième anniversaire de M. L. Rédei:

Benado, M. Sur une propriété d'interpolation remarquable dans la théorie des ensembles partiellement ordonnés.

Bruck, R. H. Sums of normal endomorphisms. II.

Daróczy, Z. Notwendige und hinreichende Bedingungen für die Existenz von nichtkonstanten Lösungen linearer Funktionalgleichungen.

Grell, H. Ein Satz über reguläre Primideale in Ringen algebraischer Zahl- und Funktionenkörper einer Veränderlichen.

Huppert, B. Subnormale Untergruppen und p-Sylowgruppen.

Pollák, G. Über die Struktur kommutativer Hauptidealringe.

Steinfeld, O. Die einstufig nichtregulären bzw. nichtprimen Ringe.

Surányi, J. Über zerteilte Parallelogramme.

Szász, F. Die Ringe mit lauter isomorphen nichttrivialen endlich erzeugbaren Unterringen.

ACTA SCIENTIARUM MATHEMATICARUM

SZEGED (HUNGARIA), ARADI VÉRTANÚK TERE 1.

Prix d'abonnement pour l'étranger $ 8.50. On peut s'abonner à l'entreprise de commerce des livres et journaux „Kultúra" (Budapest, VI., Népköztársaság útja 21).

Formátum B/5.
Terjedelem 22 (A/5) iv.
Példányszám 670.

Felelős szerk.: Szőkefalvi-Nagy Béla.
Nyomdábaadás ideje: 1960. V. 9.
Megjelenés: 1960. XI. 10.

Kiadja a Tankönyvkiadó Vállalat, Budapest, V., Szalay-u. 10—14.
Kiadásért felel a Tankönyvkiadó Vállalat igazgatója.

Szegedi Nyomda Vállalat 60-2119

INDEX — TARTALOM